VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

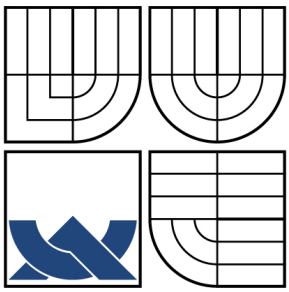
KRYPTOGRAFICKÉ MODULY PRO ZABEZPEČENÍ SÍTÍ

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

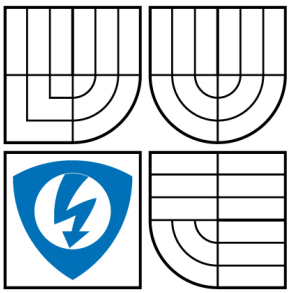
LUKÁŠ TENORA

BRNO 2008



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

KRYPTOGRAFICKÉ MODULY PRO ZABEZPEČENÍ SÍTÍ

CRYPTOGRAPHIC MODULES FOR NETWORK PROTECTION

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

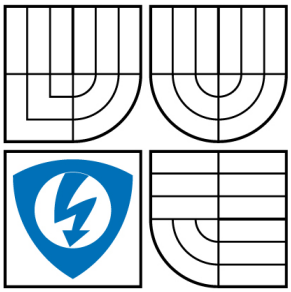
AUTOR PRÁCE — LUKÁŠ TENORA

AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. VÁCLAV ZEMAN, Ph.D.

SUPERVISOR

BRNO 2008



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student:	Tenora Lukáš	***ID:***	78419
Ročník:	3	***Akademický rok:***	2007/2008

NÁZEV TÉMATU:

Kryptografické moduly pro zabezpečení sítí

POKYNY PRO VYPRACOVÁNÍ:

Prostudujte a popište šifrovací metody používané pro zabezpečení počítačových sítí. Uveďte používané šifrovací algoritmy, autentizační metody a zhodnoťte jejich vlastnosti z hlediska zabezpečení proti nežádoucím útokům. Navrhněte a popište koncepci konkrétního řešení kryptografického zabezpečení lokální počítačové sítě.

DOPORUČENÁ LITERATURA:

[1] DOSEDĚL, T. Počítačová bezpečnost a ochrana dat. Computer Press, Brno 2003, ISBN: 80-251-0106-1.
[2] DOSTÁLEK, L. Velký průvodce protokoly TCP/IP - Bezpečnost. Computer Press, Praha 2001.

Termín zadání:	11.2.2008	***Termín odevzdání:***	4.6.2008

Vedoucí práce: doc. Ing. Václav Zeman, Ph.D.

prof. Ing. Kamil Vrba, CSc.
předseda oborové rady

UPOZORNĚNÍ:

LICENČNÍ SMLOUVA
POSKYTOVANÁ K VÝKONU PRÁVA UŽÍT ŠKOLNÍ DÍLO

uzavřená mezi smluvními stranami:

1. Pan/paní

Jméno a příjmení: Lukáš Tenora
Bytem: Vrbenského 15 717/15, 62400, Brno - Komín
Narozen/a (datum a místo): 1.3.1985, Boskovice

(dále jen "autor")

a

2. Vysoké učení technické v Brně

Fakulta elektrotechniky a komunikačních technologií
se sídlem Údolní 244/53, 60200 Brno 2
jejímž jménem jedná na základě písemného pověření děkanem fakulty:
prof. Ing. Kamil Vrba, CSc.

(dále jen "nabyvatel")

Článek 1
Specifikace školního díla

1. Předmětem této smlouvy je vysokoškolská kvalifikační práce (VŠKP):
   - ☐ disertační práce
   - ☐ diplomová práce
   - ☑ bakalářská práce

   jiná práce, jejíž druh je specifikován jako .....

(dále jen VŠKP nebo dílo)

Název VŠKP: Kryptografické moduly pro zabezpečení sítí
Vedoucí/školitel VŠKP: doc. Ing. Václav Zeman, Ph.D.
Ústav: Ústav telekomunikací
Datum obhajoby VŠKP: .....

VŠKP odevzdal autor nabyvateli v:

- ☑ tištěné formě - počet exemplářů 1
- ☑ elektronické formě - počet exemplářů 1

2. Autor prohlašuje, že vytvořil samostatnou vlastní tvůrčí činností dílo shora popsané a specifikované. Autor dále prohlašuje, že při zpracovávání díla se sám nedostal do rozporu s autorským zákonem a předpisy souvisejícími a že je dílo dílem původním.
3. Dílo je chráněno jako dílo dle autorského zákona v platném znění.
4. Autor potvrzuje, že listinná a elektronická verze díla je identická.

Článek 2

Udělení licenčního oprávnění

1. Autor touto smlouvou poskytuje nabyvateli oprávnění (licenci) k výkonu práva uvedené dílo nevýdělečně užít, archivovat a zpřístupnit ke studijním, výukovým a výzkumným účelům včetně pořizovaní výpisů, opisů a rozmnoženin.
2. Licence je poskytována celosvětově, pro celou dobu trvání autorských a majetkových práv k dílu.
3. Autor souhlasí se zveřejněním díla v databázi přístupné v mezinárodní síti
   - ☑ ihned po uzavření této smlouvy
   - ☐ 1 rok po uzavření této smlouvy
   - ☐ 3 roky po uzavření této smlouvy
   - ☐ 5 let po uzavření této smlouvy
   - ☐ 10 let po uzavření této smlouvy

   (z důvodu utajení v něm obsažených informací)
4. Nevýdělečné zveřejňování díla nabyvatelem v souladu s ustanovením § 47b zákona č. 111/1998 Sb., v platném znění, nevyžaduje licenci a nabyvatel je k němu povinen a oprávněn ze zákona.

Článek 3

Závěrečná ustanovení

1. Smlouva je sepsána ve třech vyhotoveních s platností originálu, přičemž po jednom vyhotovení obdrží autor a nabyvatel, další vyhotovení je vloženo do VŠKP.
2. Vztahy mezi smluvními stranami vzniklé a neupravené touto smlouvou se řídí autorským zákonem, občanským zákoníkem, vysokoškolským zákonem, zákonem o archivnictví, v platném znění a popř. dalšími právními předpisy.
3. Licenční smlouva byla uzavřena na základě svobodné a pravé vůle smluvních stran, s plným porozuměním jejímu textu i důsledkům, nikoliv v tísni a za nápadně nevýhodných podmínek.
4. Licenční smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.

V Brně dne: .....

....

Nabyvatel Autor

ABSTRAKT

Práce se zabývá problematikou virtuálních privátních sítí (VPN) a autentizace. V první části jsou vysvětleny moderní kryptografické metody, problematika autentizace, autentizační předměty a také problematice VPN. V druhé části práce je popsán návrh a realizace vlastní bezpečné sítě založené na technologiích firmy SafeNet.

KLÍČOVÁ SLOVA

Bezpečnost, certifikační autorita, certifikát, VPN, PKI, SafeNet.

ABSTRACT

This work deals with virtual private network (VPN) and authentication. The first section gives the modern cryptographic methods, the work of dealing with problems of authentication and authentication of objects and the issue of VPN. The second part describes the implementation of its own secure network-based technology company SafeNet.

KEYWORDS

Security, Certification Authority, Certificate, VPN, PKI, SafeNet.

TENORA L. *Hardwarové kryptografické moduly pro zabezpečení sítí.* Brno: Vysoké učení technické. Fakulta elektrotechniky a komunikačních technologií. Ústav telekomunikací, 2008. 62 s., 0 s. příloh. Bakalářská práce. Vedoucí práce byl Doc. Ing. Václav Zeman, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma Hardwarové kryptografické moduly pro zabezpečení sítí jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne 4. Června 2008

Lukáš Tenora
(podpis autora)

PODĚKOVÁNÍ

Děkuji vedoucímu bakalářské práce Doc. Ing. Václavu Zemanovi, Ph.D. za velmi užitečnou metodickou pomoc a cenné rady při zpracování bakalářské práce.

V Brně dne 4. Června 2008 Lukáš Tenora

(podpis autora)

SEZNAM ZKRATEK

AES	Advanced Encryption Standard (Pokročilý šifrovací standard)
AMC	Administrative Management Center (Administrativní řídící centrum)
CA	Certification Authority (Certifikační autorita)
CRL	Certificate revocation list (Seznam odvolaných certifikátů)
DER	Distinguished Encoding Rules (Význačné kódovací pravidlo)
DES	Data Encryption Standard (Standard pro šifrování dat)
DOS	Denial of Service (Odepření služeb)
DSA	Digital Signature Algorithm (Algoritmus digitálního podpisu)
FIPS	Federal Information Processing Standard (Federální standard pro zpracování informací)
HSM	Hardware Security Module (Hardwarový kryptografický modul)
IPSEC	Internet Protocol Security (Zabezpečení IP protokolu)
L2TP	Layer Two Tunelling Protocol (Tunelovací protokol na druhé vrstvě)
MD5	Message-Digest algorithm 5 (Algoritmus pro zpracování zpráv č. 5)
PED	Pin Entry Device (Zařízení pro zadávání PINu)
PIN	Personal Identification Number (Osobní identifikační číslo)
PKCS	Public Key Cryptography Standard (Kryptografický standard veřejného klíče)
PKI	Public Key Infrastructure (Infrastruktura veřejného klíče)
PPTP	Point to Point Tunelling Protocol (Tunelovací protokol pro spojení bod-bod)
PSK	Pre-Shared Key (Předsdílený klíč)
SHA	Secure Hash Algorithm (Bezpečný hashovaní algoritmus)
SMC	Security Management Center (Centrum pro správu bezpečnosti)
SSL	Secure Sockets Layer (Vrstva bezpečných soketů)
SSO	Single Sign-On (Jednotné přihlášení)
VPN	Virtual Private Network (Virtuální privátní síť)

OBSAH

SEZNAM OBRÁZKŮ

ÚVOD

Cílem práce bylo rozebrat problematiku sítové bezpečnosti a to se zaměřením na autentizaci. Teoretická část práce je věnována problematice moderní kryptografie a jejím využití při zabezpečení počítačových sítí. Dále je pozornost zaměřena na problematiku certifikační autority, která je důležitým prvkem při vytváření kryptograficky zabezpečeným sítím. Věnoval jsem se také zabezpečení certifikační autority prostřednictvím hardwarových kryptografických modulů. Na závěr jsem rozebral problematiku virtuálních privátních sítí.

V praktické části jsem se věnoval řešením virtuálních privátních sítí za pomoci technologií společnosti SafeNet a problematice autentizace za použití technologie Borderless Security téže firmy.

1 KRYPTOGRAFIE

Kryptografie je vědní obor, zabývající se utajováním dat pomocí šifrování. Šifrováním se rozumí proces, kdy za pomoci šifrovacího algoritmu a klíče se data transformují z otevřené podoby do podoby utajené, šifrované. Kryptografické metody poskytují pro zabezpečení dat následující služby:

- **Důvěrnost**, zabezpečuje utajení informace před neoprávněnými uživateli.
- **Autentičnost**, příjemce zprávy má možnost zjistit její původ, zamezení případným narušitelům vydávat se za někoho jiného.
- **Integritu**, kontrolu zprávy zda nebyla během přenosu modifikována.
- **Nepopiratelnost** odesílatel by neměl mít možnost popřít, že danou zprávu odeslal.

K zajištění uvedených služeb využívá kryptografie následujících prostředků:

- Symetrické a asymetrické šifrovací algoritmy
- Hašovací funkce
- Digitální podpis
- Kryptografické protokoly a další.

1.1 Symetrická kryptografie

Algoritmy patřící do kategorie symetrické kryptografie používají jeden tajný klíč pro obě šifrovací operace, tzn., že jediným tajným klíčem data šifrujeme i dešifrujeme. Hlavní výhoda symetrické kryptografie je rychlost, nevýhodou je však složitější distribuce klíče.

1.1.1 Algoritmus 3DES

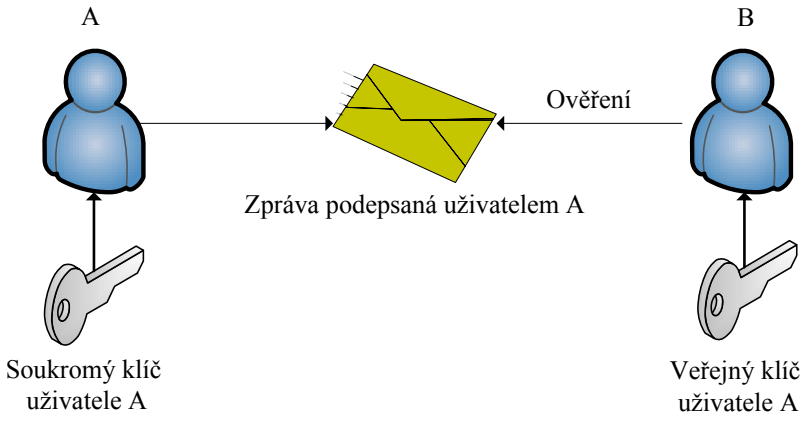
Jedná se o symetrický šifrovací algoritmus, který nahradil nedostačující 56 bitový algoritmus DES. Algoritmus 3DES není nic jiného, než 3x DES za sebou, přičemž mohou být použity 2 klíče, v tom případě se jedná o 112 bitovou variantu, nebo může být každý klíč jiný, potom se jedná o 168 bitovou variantu. Nevýhodou algoritmu 3DES je jeho rychlost, protože aplikováním tří algoritmů DES za sebou se také třikrát snížila jeho rychlost. Dnes byl již algoritmus nahrazen podstatně rychlejším a bezpečnější algoritmem AES.

1.1.2 Algoritmus AES

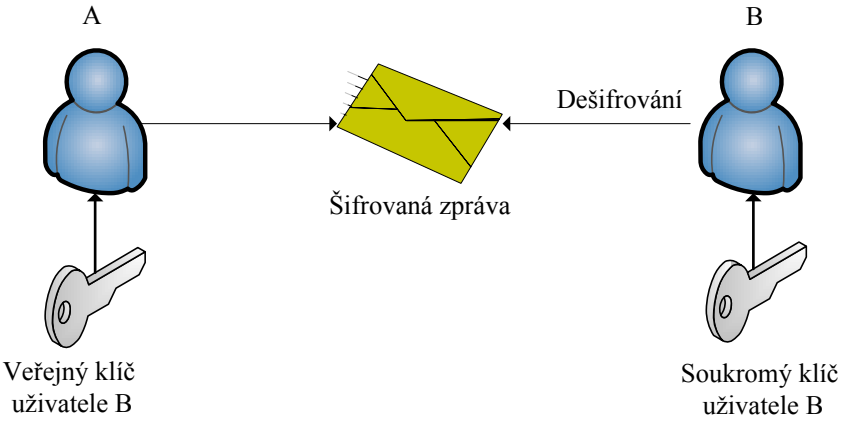
Algoritmus AES je taktéž symetrický šifrovací algoritmus, který nahradil již nedostačující algoritmus DES. Vznikl v roce 2001 po vyhlášení veřejné soutěže, kterou vyhrála šifra Rijndael, jehož tvůrci byli Joan Daemen a Vincent Rijmen. Ten byl přijat americkým Národním institutem pro standardizaci a technologie (NIST) pod názvem AES.
AES je iterovaná bloková šifra s délkou bloku 128 bitů, která používá délku klíčů 128, 192 nebo 256 bitů. AES pracuje v rundách, jejichž počet je 10, 12 nebo 14 v závislosti na délce klíče. Jedná se o velmi rychlou šifru s minimálními nároky na výpočetní výkon a paměť.

1.2 Asymetrická kryptografie

Asymetrická kryptografie se vyznačuje existencí dvou klíčů, tzv. klíčového páru. Jeden klíč je tzv. soukromý a slouží k podepisování a dešifrování dat. Druhý je tzv. veřejný a slouží k ověření podpisu a k šifrování.



Obr. 1.2.1: Proces podepisování



Obr. 1.2.2: Proces šifrování

1.2.1 Algoritmus RSA

Jedná se o asymetrický šifrovací algoritmus, který byl pojmenován po svých tvůrcích, kterými byli Ronald Rivest, Adi Shamir a Leonard Aleman. Výhodou oproti symetrickým šifrovacím algoritmům je, že řeší problém distribuce klíč ovšem za cenu značné výpočetní náročnosti. Nejlepším řešením je použití hybridního šifrování, které kombinuje obě možnosti – velkou zprávu zašifrujeme rychlou symetrickou šifrou a její klíč následně pomocí asymetrického šifrování. Při volbě délky klíče bychom měli brát v úvahu jeho využití. Klíče o délce 512 bitů byly prolomeny útoky hrubou silou již v roce 1997, proto je doporučeno používat minimálně 1024 bitů, pro větší bezpečnost pak 2048, či 4096 bitů. Nevýhodou delších klíčů je fakt, že s dvojnásobnou velikostí klíče roste doba generování zhruba 16x a doba nutná pro dešifrování a šifrování 8x resp. 4x. Alternativou RSA je DSA, který není svázán licenčními podmínkami.

1.3 Digitální otisk dat

Digitální otisk dat (hash) slouží k jednoznačnému určení vstupních dat na základě jejich digitálního otisku. Hashovací algoritmus nám umožňuje převod vstupního řetězce dat proměnlivé délky na výstupní řetězec pevné délky. Hash se používá k ukládání hesel, ke kontrole integrity souborů a také při digitálním podpisu.

Požadavek na bezpečnou hashovaní funkci je, aby byla jednocestná, tj. aby nebylo možné z hashe získat zpět původní zprávu a bezkolizní. Protože hash má konečnou hodnotu např. MD5 maximálně 2^{128} kombinací, ale vstupních zpráv je nekonečně mnoho, je tedy důležité, aby neexistoval algoritmus, díky kterému by bylo možné najít dvě zprávy se stejným hashem.

Útoky za účelem získání vstupního řetězce, především přihlašovacího hesla, na základě otisku jsou následující:

- **Útok hrubou silou (Brutal-force attack)** Tento způsob je založen na testování všech možných řetězců dané délky a znakové sady. To znamená, že pokud by bylo heslo složeno z písmen malé abecedy a čísel o délce max. 5 znaků, máme $36^1+36^2+36^3+36^4+36^5+36^6$ kombinací. Vytvoříme hash ke každé kombinaci a ten porovnáme s hashem, který chceme prolomit. Proto je dobré volit dlouhá hesla za použití všech možných znaků.

- **Slovníkový útok (Dictionary attack)** Tento způsob je založen na tom, že máme slovník se slovy, ke kterým jsou přiřazeny hashe, útok pak jako v předešlém případě porovnává hash s tou ve slovníku. Tento způsob je ovšem spíše teoretický, protože spousta aplikací zabraňuje použití známého slova jako hesla, nebo na to alespoň upozorní.

- **Rainbow tables** V tomto případě máme předgenerovanou tabulku hashů k daným heslům, ve které se potom vyhledává. Nevýhodou je ovšem značná velikost tabulky (až několik desítek GB).

Jedním z možných způsobů, jak se chránit před slovníkovými útoky, je použití tzv. „solení hashů“. To znamená, že se na vstup k heslu přidá ještě náhodný řetězec, který je pokaždé jiný, což má za následek, že dvě stejná hesla mají dva rozdílné hashe, a tak při prolomení hesla jednoho uživatele nejsou ohroženi ostatní, kteří použili stejné heslo.

1.3.1 MD5

MD5 (Message Digest Algorithm 5) je kryptografická hashovací funkce, která vrací digitální otisk ze vstupu o velikosti 128 bitů. V dnešní době se již nepoužívá. Protože v roce 2004 byly objeveny zásadní chyby v jejím návrhu čínským týmem Dr. Wangové a později českým kryptologem Vlastimilem Klímou, který objevil algoritmus, díky kterému je možné nalézt kolizi zhruba za 2 minuty.

1.3.2 SHA

SHA (Secure Hash Algorithm) je kryptografická hashovací funkce, která vrací digitální otisk ze vstupu o velikosti 160 bitů, tato varianta se označuje jako SHA-1, nebo o velikosti 256 až 512 bitů a ta se označuje jako SHA-2. Algoritmus SHA je využit v bezpečnostních aplikacích a protokolech, jako jsou např. TLS, SSL, PGP, SSH a IPSec. U algoritmu SHA-1 byla také nalezena kolize, ovšem v tomto případě není problém závažný, jelikož její nalezení je časově náročné a trvá 1-2 měsíce. S současné době se připravuje nový algoritmus SHA-3, která nebude vázána žádnými autorskými právy a bude schopna po desetiletí udržet v bezpečí citlivé informace. Algoritmus SHA-3 by měl mít stejnou výstupní velikost jako SHA-2, ale měl by obsahovat určitá bezpečnostní a výkonová vylepšení.

Tab. 1.3.1 Porovnání jednotlivých verzí algoritmů SHA

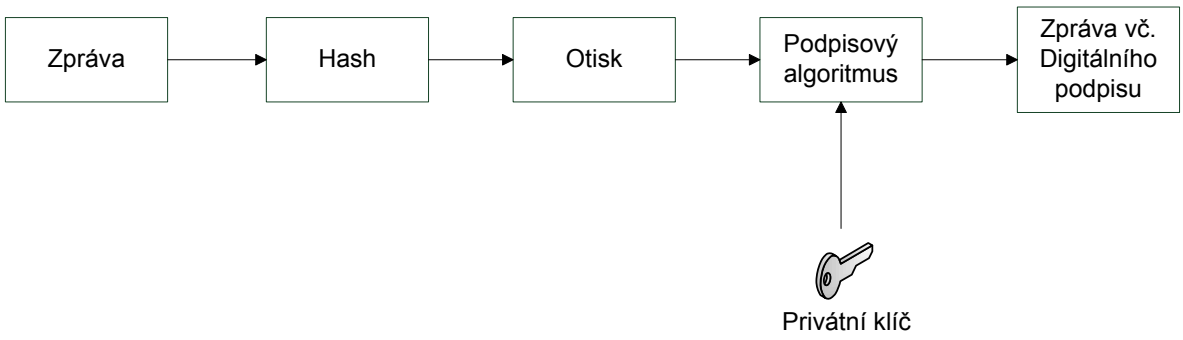
Algoritmus	Výstupní velikost (bit)	Velikost bloku (bit)	Max. velikost zprávy (bit)	Délka slova (bit)	Kolize
SHA-0	160	160	2^{64}-1	32	Ano
SHA-1	160	160	2^{64}-1	32	Ano
SHA-256/224	256/224	512	2^{64}-1	32	Ne
SHA-512/384	512/384	1024	2^{128}-1	64	Ne

1.4 Digitální podpis

Digitální podpis slouží k zajištění autentičnosti a nepopiratelnosti přijatých zpráv. Digitální podpis umožňuje jednoznačně identifikovat podepisujícího a navíc umožňuje zajistit integritu přenášených dat.

1.4.1 Vytvoření digitálního podpisu

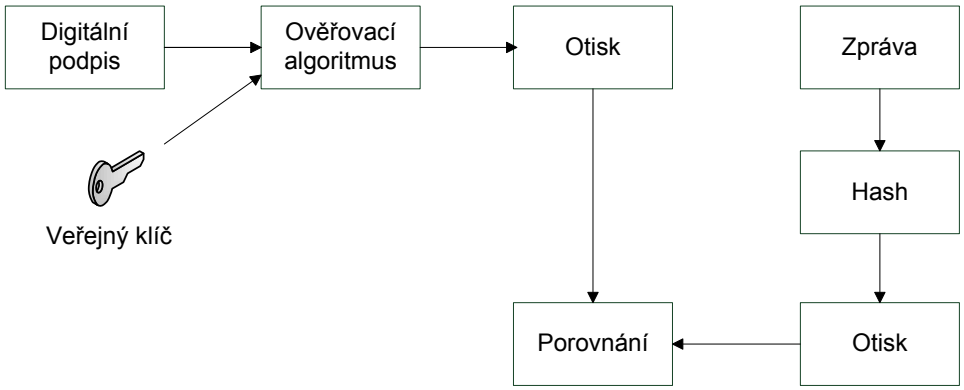
Digitální podpis se vytváří na základě asymetrického algoritmu šifrou privátního klíče. Abychom ale nemuseli podepisovat celou zprávu pomalou asymetrickou šifrou, vytvoří se nejdříve digitální otisk zprávy (hash) a ten se teprve podepíše privátním klíčem a asymetrickým algoritmem.



Obr. 1.4.1: Princip vytvoření digitálního podpisu

1.4.2 Ověření digitálního podpisu

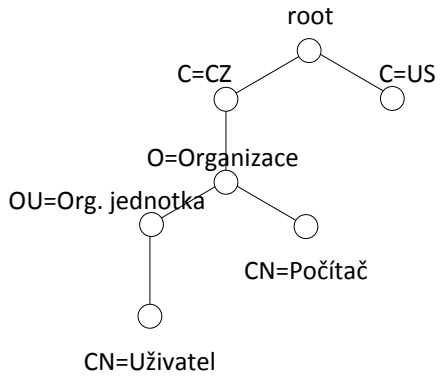
Při ověřování digitálního podpisu porovnáváme, zdali nebyla zpráva cestou pozměněna. Vytvoříme digitální otisk zprávy a ten porovnáme s otiskem, který získáme z digitálního podpisu.



Obr. 1.4.2: Princip ověření digitálního podpisu

1.5 Distribuce veřejného klíče

Distribuce veřejného klíče řeší problém identifikace vlastníka veřejného klíče a jeho jednoznačného určení. V předchozí kapitole jsme si ukázali, že pomocí veřejného klíče lze ověřit platnost digitálního podpisu. Nyní ovšem potřebujeme ověřit, že veřejný klíč je skutečně klíčem daného uživatele. K tomu slouží certifikát veřejného klíče, který je podepsaný důvěryhodnou certifikační autoritou. Formát certifikátů je dán normou ITU-T X.509, který definuje jeho formát a jeho záznamy řadí do stromové struktury, jak je znázorněno na obr. 1.5.1.



Obr. 1.5.1: Struktura záznamů X. 509

Certifikátu podle normy X. 509 obsahuje následující záznamy:

- Verze
- Sériové číslo
- Identifikátor algoritmu
- CA
- Doba platnosti certifikátu
- Subjekt (jméno uživatele, kterému patří certifikovaný veřejný klíč)
- Veřejný klíč
- Podpis CA

Existují různé formáty certifikátů:

- **Binární X.509 – kódování DER (Distinguished Encoding Rules)** se používá se pro zakódování dat před jejich podepsáním. Má příponu .DER

- **X.509 – kódování Base64** Jedná se o kódovací algoritmus, který zakóduje binární data v běžně tisknutelné znaky ASCII (Velká a malá písmena, číslice, znak plus a lomítko). Byl navržen pro použití se standardem S/MIME (Secure/Multipurpose Internet Mail Extensions), který se používá pro přenos binárních příloh přes síť internet. Výhodou tohoto kódování je snadná přenositelnost. Má příponu .PEM. Údaje kódovány v Base64 mají následující formát:

  -----BEGIN CERTIFICATE-----
  MIICdjCCAd+gAwIBAgIBCDANBgkqhkiG9w0BAQUFADBXMQswCQYDVQQGEwJD
  WjELMAkGA1UECBMCQ1oxDTALBgNVBAcTBEJSTk8xDTALBgNVBAoTBFVUS08x
  DDAKBgNVBAsTA1ZVVDEPMA0GA1UEAxMGU01DIENBMB4XDTA4MDEzMDEyMj
  AyNFoXDTMzMDEzMDEyMjAyNFowbDELMAkGA1UEBhMCQ1oxCzAJBgNVBAgTAk
  NaMQ0wCwYDVQQHEwRCUk5PMQ0wCwYDVQQKEwRVVEtPMQwwCgYDVQQLEw
  NWVVQxJDAiBgNVBAMTGzAwMEQtMDAwMDAwMDEtMDAwZjVhZTEtMDAwMD
  CBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuyauZkFwIh0tRU5EjtAKEj34pyRa
  D7+E9MCEQSpllRimh1GyKmK7aOb6WRCd1JHOJ8kBNeSbwiXvMbEiOTs6MahdHu7V6
  yvHC3B0BR97CgT8zzk+YfrJPFfWHObAY4VS/8u3adsCxSYCe20XWiO3brCp/sc4bCeJgth
  OL2axfG8CAwEAAaM9MDswOQYDVR0RBDIwMIcECgAAb4EXc3VwcG9ydEBzYWZlb
  mV0LWluYy5jb22CD3NhZmVuZXQtaW5jLmNvbTANBgkqhkiG9w0BAQUFAAOBgQB7
  oG9IiS3S9SaUDmNxvbO3cSr/aZcgBAKFqvRik6Aq5w4PgBCIWAd1fERZaNa35nZrY0MU
  XwjNr7mp2OoZPHH2eDX0wof4DmvzpAjmzh19VFQ64E7lcMyUqePh4vGkfveNiu0t4Ae1
  XeFH6wIEvHMsJPbl9ii5uGtyx9umCjLwZw==
  -----END CERTIFICATE-----

- **PKCS#7 (Public Key Cryptography Standard, RFC 2315)** Tento formát umožňuje přenos certifikátů z jednoho počítače na druhý, či na vyměnitelné medium. Je kompatibilní se standardem ITU-T X. 509. Má příponu.P7B

- **PKCS#12 (Public Key Cryptography Standard)** Tento formát umožňuje také přenos certifikátů z jednoho počítače na druhý a dále je vhodný k záloze certifikátů včetně soukromého klíče. Má příponu .PFX nebo .P12

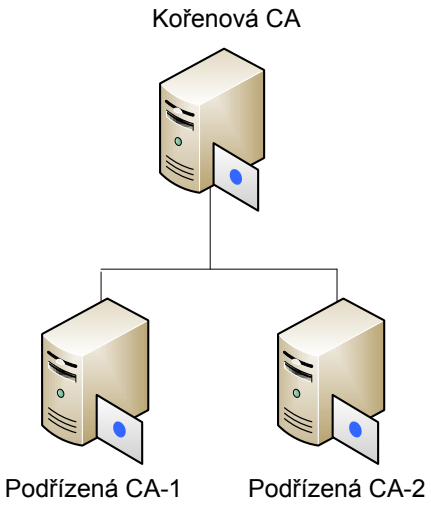
1.6 Certifikační autorita

Certifikační autorita je hlavní prvek infrastruktury veřejného klíče – PKI (viz lit. [3]). Certifikační autorita má následující úkoly:

- Vydávání certifikátů
- Ověření identity žadatele o certifikát
- Podepsání certifikátu pro žadatele o certifikát
- Správa zrušených certifikátů

1.6.1 Typy certifikačních autorit

Ve velkých společnostech bývá více certifikačních autorit, které jsou řazeny do hierarchie, která se skládá z kořenové CA, a několika podřízených CA viz obr. 7.1. Kořenová CA vydává certifikáty podřízeným CA v hierarchii a ty pak vydávají certifikáty pro uživatele, počítače, či sítové prvky. Zpravidla platí, že privátní klíče CA na vyšších úrovních hierarchie mají delší životní cyklus a v případě kořenové CA také délku až 4096 bitů, na rozdíl od podřízených CA, kde je doporučeno používat délku klíče 2048 bitů.



Obr. 1.6.1: Názorná ukázka hierarchie certifikačních autorit

Operační systém Microsoft Windows Server 2003 v sobě integruje několik typů certifikační autority:

- **Kořenová certifikační autorita rozlehlých sítí**, jedná se o hlavní CA v rozsáhlé síti, integrována v Active Directory. Certifikáty se vydávají na základě definovaných šablon.
- **Podřízená certifikační autorita rozlehlých sítí**, spadá pod kořenovou CA, kterou potřebuje pro svoji funkci.
- **Samostatná kořenová certifikační autorita**, je určena pro střední a menší firmy, nevyžaduje Active Directory.
- **Samostatná podřízená certifikační autorita**, spadá pod samostatnou kořenovou CA, kterou potřebuje pro svoji funkci.

V našem projektu jsme využili samostatné kořenové autority, jejíž privátní klíč chránil kryptografický modul Luna PCI, k vydání certifikátů na základě žádosti pro ověření stanice

přes VPN. Samostatná CA byla zvolena proto, že nevyužívá šablony certifikátů, které nevyhovovaly naší žádosti.

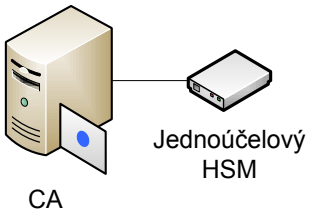
1.6.2 Zabezpečení certifikační autority

Zabezpečením certifikační autority rozumíme především ochranu jejího soukromého klíče. K tomu nám slouží hardwarové kryptografické moduly, označované též zkratkou HSM. Soukromý klíč je v takovém případě vygenerován pomocí modulu a bezpečně uložen do jeho paměti, ze které jej nelze exportovat a tím zabránit jeho případného zneužití.

Hardwarové kryptografické moduly jsou hardwarová zařízení v podobě externích modulů, či PCI karet, které slouží ke generování, uchovávání a ochraně klíčů a dále akceleraci kryptografických operací. Úroveň bezpečnosti HSM definuje sada norem FIPS 140. Kryptografický modul se skládá z mikroprocesoru, kryptografického koprocesoru, který urychluje kryptografické operace, paměti a ze senzorů průniku, které detekují, zdali se někdo snaží dostat do modulu a v závislosti na tom mohou vyvolat určitou reakci (např. smazání obsahu paměti).

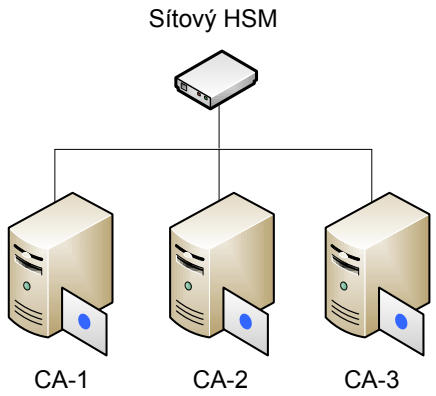
Kryptografické moduly řadíme do dvou kategorií:

- **Jednoúčelové kryptografické moduly (Dedicated HSM)**, jsou připojeny k CA přímo přes rozhraní PCI (či PCI-X), nebo přes rozhraní SCSI.



Obr. 1.6.2: Jednoúčelový HSM

- **Sítové kryptografické moduly (Network-Attached HSM)**, jsou připojeny do počítačové sítě a umožňují tak spolupráci s více CA.



Obr. 1.6.3: Sítový HSM

Jak již bylo řečeno, úroveň bezpečnosti kryptografických modulů definuje americký federální standard FIPS 140, který je určen pro kryptografické moduly. Zahrnuje jednak hardwarovou, tak i softwarovou část modulu. Podle nároků na bezpečnost je rozdělen do 4 úrovní:

- **Level 1** definuje základní bezpečnostní požadavky, jako je např. použití schválených kryptografických algoritmů apod.
- **Level 2** klade nároky na evidenci průniku, autentizace je závislá na rolích.
- **Level 3** klade nároky na evidenci průniku a odezvu (destrukce citlivých dat apod.), autentizace je založená na identitách.
- **Level 4** definuje nejsilnější bezpečnostní opatření. Protože se předpokládá použití v nezabezpečených prostorech, požaduje silnou fyzickou ochranu a dodržování vnějších pracovních podmínek.

2 AUTENTIZACE

Autentizace je jedna ze základních funkcí, kterou lze zabezpečit pomocí moderních kryptografických prostředků. Umožňuje vzájemné ověření dvou komunikujících stran (viz lit. [1]).

2.1 Autentizační protokoly

Autentizační protokoly používáme k ověření identity uživatele, či systému. Využívají se k tomu kryptografické prostředky uvedené v předchozí kapitole. Mezi nejpoužívanější autentizační protokoly patří:

- **Kerberos** jedná se o síťovou autentizaci a dále autentizace mezi uživatelem a serverem.
- **SSL/TLS** sítová autentizace založená na certifikátech
- **NTLM** sítová autentizace
- **MS CHAP** síťová autentizace, používá se při spojení bod-bod
- **EAP** to samé co MS CHAP s podporou čipových karet SmartCard
- **EAP-TLS** autentizace používaná u bezdrátového připojení
- **RADIUS** jedná se o protokol pro vzdálené přihlašování
- **DIAMETER** protokol pro vzdálené přihlašování nahrazující RADIUS
- **IEEE 802.1X** standard pro řízení přístupu, využívá se k autentizaci zařízení v lokálních sítích LAN.

2.1.1 NT LAN Manager (NTLM)

Protokol NTLM používán staršími operačními systémy (Windows 9x, NT, DOS, OS/2) pro autentizaci. Je nutný pro sítovou autentizaci, pokud jsou v síti stanice s Windows NT 4.0, které nepodporují Kerberos.

2.1.2 Kerberos

Je autentizační protokol (viz lit. [13]), který vznikl již v roce 1987 jako KerberosV4, druhá verze byla specifikována v roce 1993 a uvolněna o 3 roky později. Protože byly v USA problémy s vývozem kryptografie, vnikla volně šiřitelná verze Heimdal pro Evropu, která je samozřejmě kompatibilní.

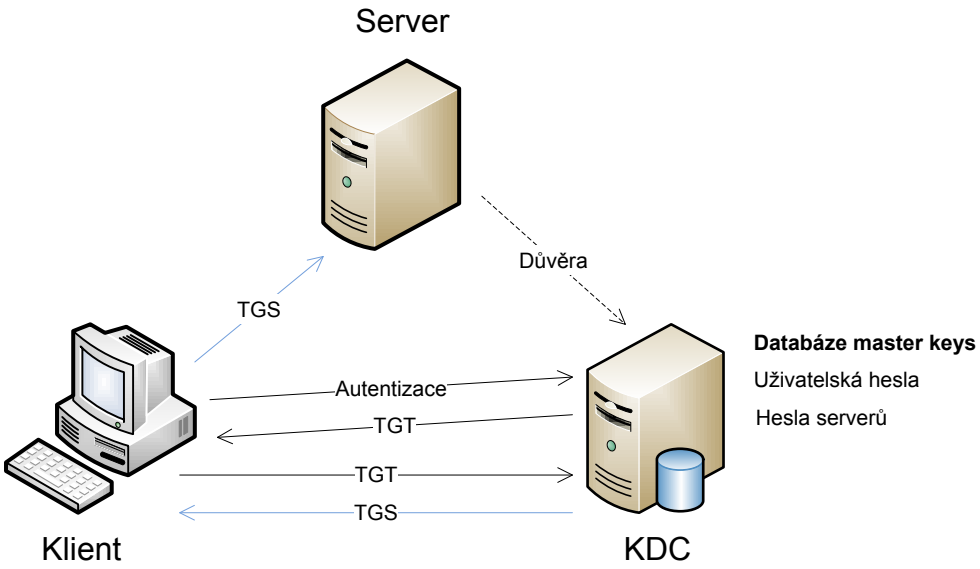
Autentizace uživatelů je založena na důvěryhodné třetí straně, která je tvořena centrem distribuce klíčů (KDC). Centrum distribuce klíčů přiděluje tzv. tikety, které prokazují identitu uživatele a neobsahují žádné citlivé informace. Tiket je nutný pro každou službu zvlášť a jeho platnost je časově omezena.

Centrum distribuce klíčů se dělí na dvě logické části:

- Autentizační server (AS)
- Tiket server (TGS)

Kerberos obsahuje databázi tajných klíčů, pomocí kterých se uživatelé identifikují. Pro komunikaci mezi klientem a serverem, či klientem a KDC je při přihlášení náhodně vygenerován session key, jehož platnost je časově omezena.

Proces autentizace



Obr. 2.1.1 Proces autentizace Kerberos

1. Uživatel zadá svůj login a heslo, ze kterého se hashovaní funkcí vypočítá master key (MK). Počítač pošle žádost autentizačnímu serveru (AS), tato komunikace je nešifrovaná a obsahuje pouze login uživatele a master key. Autentizační server v databázi vyhledá uživatele s daným loginem a pošle uživateli zašifrovaný TGT tiket a klient-TGS session key.

2. Uživatel pošle žádost na tiket server (TGS) o tiket, šifrovanou pomocí klient-TGS session key. Server žádost dešifruje a pošle uživateli klient-server tiket a klient-server session key.

3. Klient pošle serveru šifrovaný klient-server tiket a nový autentifikátor, který obsahuje ID klienta a timestamp. Server dešifruje tiket a potvrdí svou identitu, pošle také timestamp inkrementovaný o 1. Klient zprávu dešifruje, ověří timestamp a pokud je v pořádku, může důvěřovat danému serveru a využívat jej.

Zranitelnost Kerbera

Kerberos je rozsáhlý autentizační protokol s řadou bezpečnostních prvků, ale stejně jako každý jiný protokol má i Kerberos své slabiny.

Pokud se podaří útočníkovi odchytit část komunikace, je schopen se identifikovat jako legitimní účastník (tento problém byl vyřešen použitím časových známek - timestamp).
Dále je možné pomocí slovníkového útoku odhalit jednoduchá hesla uživatelů pokud je zachycena část komunikace obsahující Master key. Tomuto útoku se lze bránit použitím bezpečných hashovacích algoritmů.

2.1.3 RADIUS

Jedná se o protokol pro vzdálené přihlašování, kdy se vzdálení uživatelé přihlašují na NAS (Network Access Server), který dále předá informace (nejčastěji login a heslo) RADIUS serveru, který ověří jejich identitu pomocí autentizačního protokolu (např. CHAP). Pro zabezpečení přihlašovacích údajů nejsou posílány v textové podobě, ale v podobě hashe. Po úspěšné autentizaci je vzdálenému účastníkovi přidělena IP adresa, šířka pásma atd.
RADIUS je využíván v protokolu 802.1x, který se velmi často využívá v bezdrátové LAN. Využívá transportní protokol UDP.

2.1.4 DIAMETER

Jedná se o autentizační, autorizační a účtovací protokol, který vznikl z protokolu RADIUS. Hlavním rozdílem mezi oběma protokoly je, že DIAMETER používá transportní protokol TCP, může použít k zabezpečení sady protokolů IPSec a disponuje lepší podporou roamingu.

2.1.5 Protokol 802.1X

Jedná se o standard řízení přístupu (viz lit. [14], [15]) k sítí založený na EAP, který je využíván k autentizaci zařízení v sítích LAN. Jeho princip spočívá v tom, že připojené zařízení nepřipojí na port, dokud se neautentizuje. Protokol 802.1X umožňuje autentizaci pomocí hesel, tokenů či PKI certifikátů. Procesu autentizace se účastní tři zařízení, klient, autentizátor a RADIUS server. Funkci autentizátoru může vykonávat např. jednoduchý router či Access point, s podporou IEEE 802.1x. Komunikace mezi klientem a autentizátorem probíhá pomocí EAP protokolu a mezi autentizátorem a RADIUS serverem pomocí RADIUS protokolu. O převod protokolů se stará autentizátor.

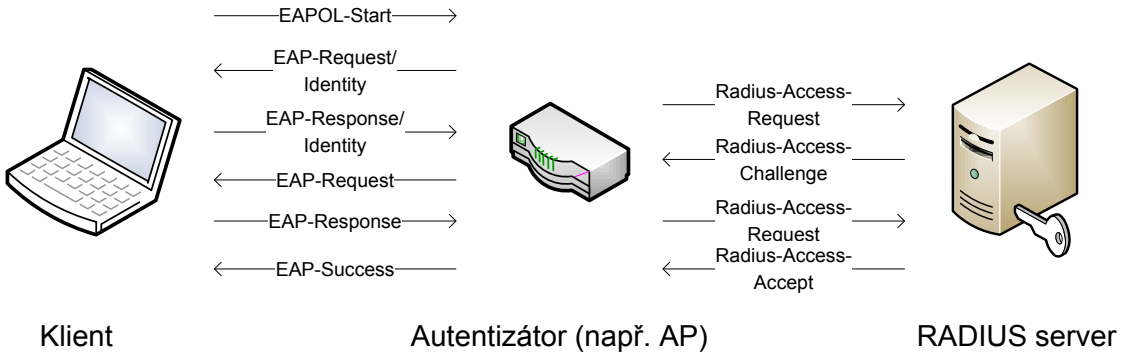
Proces autentizace:

1. Vzdálený klient odešle požadavek EAPOL-Start, že se chce připojit do sítě. Autentizátor odešle klientovi požadavek na ověření EAP-Request/Identity.

2. Vzdálený klient pošle svoje identifikační údaje (EAP-Response/Identity) na Autentizátora, který je přepošle na RADIUS server. RADIUS pošle na Autentizátora

požadavek na ověření, na který odpoví klient tím, že pošle autentizátorovi hash svého hesla.

3. Jestliže klient zašle správné údaje, je mu umožněn přístup do sítě.



Obr. 2.1.2 Proces autentizace 802.1X

Protokol 802.1x používá dynamicky se měnící klíče a tak odolává mnohým útokům, zejména útokům typu Man-in-The-Middle.

2.1.6 Autentizace v SSL

SSL je protokol pro zajištění šifrovaného TCP/IP kanálu. Autentizace probíhá nejčastěji na straně serveru (s výjimkou bankovních služeb, kde se autentizuje i uživatel). Autentizace probíhá tak, že vzdálený uživatel odešle požadavek na zabezpečený kanál. Po jeho ověření se vygeneruje klíč relace šifrovaný serverovým certifikátem a následně může probíhat šifrovaná komunikace. Protože je šifrování většího počtu SSL kanálů časově náročné, instalují se do serveru SSL akcelerátory.

2.2 Útoky na autentizační protokoly

Cílem útoků na autentizační protokoly je, aby se útočník mohl vydávat za důvěryhodnou stranu. Toho je možné dosáhnout např. odposlechem komunikace či zneužitím chyby při návrhu protokolu. Nejčastější útoky jsou:

- **Replay Attack** - Útok spočívá v odposlechu komunikace dvou autentizujících se stran a následném zneužití získaných dat pro autentizaci. Řešením proti útoku je použití časového razítka nebo metody výzva-odpověď.

- **Man-in-The-Middle Attack –** Útok spočívá v tom, že mezi oběma komunikujícími stranami se nachází útočník, jenž odposlouchává autentizaci, aby se následně mohl vydávat za důvěryhodnou stranu.

2.3 Autentizace prostřednictvím čipových karet SmartCard a USB Tokenů

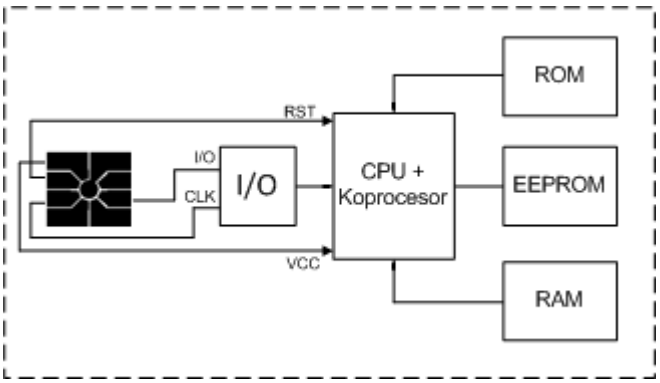
V mnohých případech je používání hesla nedostačující, mnozí uživatelé volí záměrně jednoduchá a lehce zapamatovatelná hesla, která lze prolomit slovníkovým útokem. Dalším rizikem je prozrazení hesla, nebo jeho odhalení pomocí nejrůznějších aplikací, které sledují stištěné klávesy (tzv. „keyloggery“) apod. Řešením těchto problémů může být zavedení čipové a použití tzv. dvou faktorové autentizace. Dvou faktorová autentizace používá následující kombinaci (viz lit. [3], [5]):

- Vlastnictví fyzického předmětu (USB Token, Smart Card)
- Znalost PINu pro přístup k digitálnímu certifikátu, uloženého na kartě, či tokenu.

Z výše uvedeného vyplývá, že znalost samotného PINu, nebo vlastnictví fyzického předmětu nestačí k přístupu k digitálnímu certifikátu, proto jsou čipové karty a použití dvou faktorové autentizace nedílnou součástí PKI

2.3.1 Čipové Karty SmartCard

Čipová karta SmartCard slouží k zabezpečení osobních dat (soukromé klíče, hesla apod.), která jsou uložena v její paměti. Karta obsahuje vestavěný čip, který obstarává kryptografické funkce a umožňuje vygenerovat klíčový pár, přičemž soukromý klíč nikdy neopouští paměť čipové karty. Dalším prvkem čipové karty je paměť, která slouží pro uložení osobních dat. Její kapacita se liší v závislosti na typu čipové karty a pohybuje se v rozmezí od 8kB do 64kB.



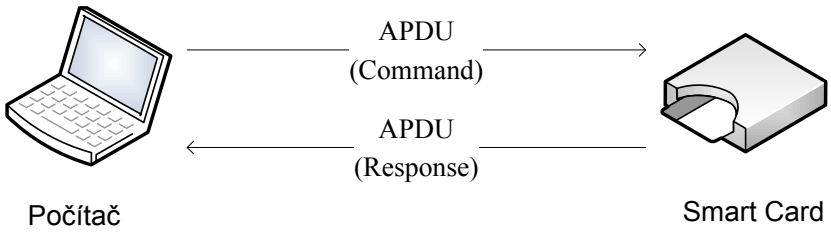
Obr. 2.3.1: Blokové schéma karty SmartCard

Čipové karty jsou standardizovány skupinou ISO/IEC. Kontaktními čipovými kartami se zabývá ISO 7816 1-6, bezkontaktními ISO/IEC 14443. ISO 7816 specifikuje:

- **ISO 7816-1** fyzickou podobu karty a to rozměry, tloušťku a odolnost v ohybu.
- **ISO 7816-2** plochu čipu a polohu kontaktů
- **ISO 7816-3** elektrické charakteristiky, napětí a proud v kontaktech
- **ISO 7816-4** charakteristiky signálové komunikace na rozhraní čipové karty, návaznost, frekvence
- **ISO 7816-5** číselné identifikátory a registrační procedury pro identifikátory aplikací
- **ISO 7816-6** Interdisciplinární datové prvky

Aplikační protokol ISO 7816-4 (APDU)

Aplikační protokol slouží k přenosu dat mezi koncovým zařízením (počítačem) a čipovou kartou Smart Card.



Obr. 2.3.2: Schéma aplikačního protokolu APDU

2.3.2 USB Tokeny

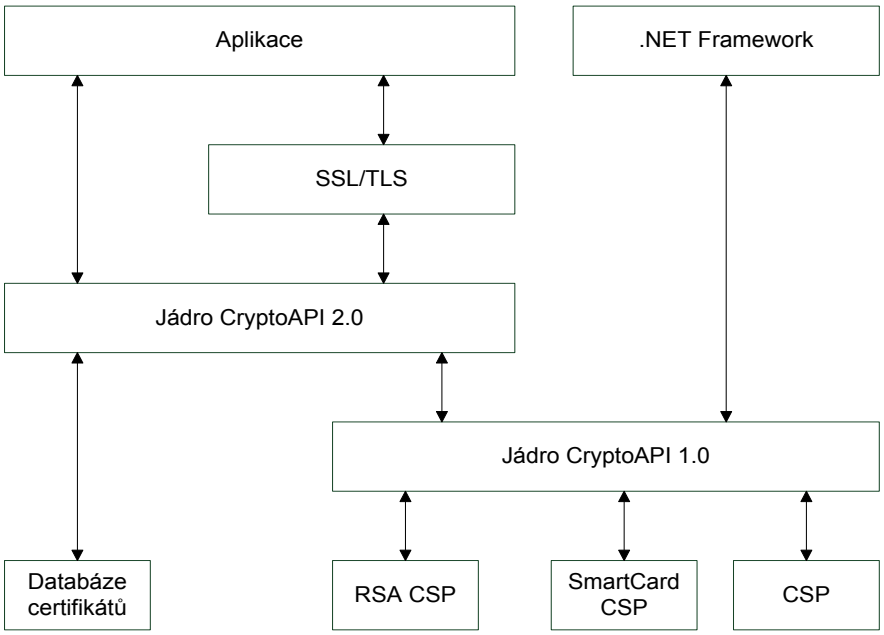
USB Tokeny jsou v podstatě jinou podobou karet SmartCard, které umožňují připojení k počítači pomocí portu USB a tak není potřeba fyzické čtečky karet. V takovém počítači se nainstaluje virtuální čtečka, ke které se připojený USB Token virtuálně připojí a tváří se tak pro operační systém jako karta SmartCard.

Některé modely, podporující FIPS 140-2 level 2 a vyšší, mají pouzdro z pryskyřice, které se při pokusu o vniknutí rozlomí na několik kusů a token je tak nenávratně zničen.

2.3.3 Rozhraní operačního systému pro přístup k autentizačním předmětům

Aby operační systém mohl přistupovat ke kartám Smart Card, či USB tokenu, je zapotřebí speciálního API, které se v operačním systému Microsoft Windows nazývá CryptoAPI. Jedná se o programátorské rozhraní, které umožňuje aplikacím šifrování, digitální podepisování dat

a zabezpečení soukromých klíčů. Kryptografické operace jsou prováděny zprostředkovateli kryptografických služeb – CSP. Jedná se o zásuvné moduly, kterými lze rozšířit CryptoAPI o podporu karet Smart Card, USB tokenů apod. daného výrobce.



Obr. 2.3.3: Schéma rozhraní operačního systému MS Windows pro přístup k autentizačním předmětům.

2.3.4 Srovnání čipových karet SmartCard a UBS Tokenů

Porovnáme-li čipové karty SmartCard a USB Tokeny, nalezneme výhody i nevýhody každého řešení. Za USB Tokeny mluví vysoká životnost konektoru a absence hardwarové čtečky, nevýhodou je ovšem nižší bezpečnost, jelikož se snazší jej rozebrat a dostat se k čipu, popř. odposlouchávat data na sběrnici a vyšší pořizovací cena. Řešení pomocí USB tokenů je vhodné, chceme-li umožnit zaměstnancům firmy vzdálený přístup z domácího počítače, na kterém bychom stěží hledali čtečku karet, nebo klientům banky pro bezpečnou správu svého účtu. Karty SmartCard potom nabízí ještě větší bezpečnost a možnost potisku (např. fotka držitele). Nevýhodou je pak nutnost hardwarové čtečky a nízká životnost, dána fyzickým opotřebením. Řešení na bázi karet je vhodné do větších firem, kde se uživatelé přihlašují ke svému počítači prostřednictvím karet.

2.3.5 Útoky na karty Smart Card a USB Tokeny

Čipové Karty Smart Card, či USB Tokeny jsou v mnoha případech považovány za bezpečné úložiště privátního klíče, protože standardními postupy jej není možné vyexportovat a v krátkém čase ani jinak získat. Možný problém může nastat v případě, dojde-li ke zcizení

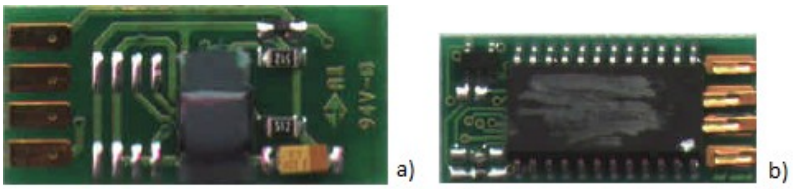
tokenu a útočník má dostatek času, aby z něj tajnou informaci získal (viz lit. [17]). Existují dva druhy útoků na zařízení:

- **Invazivní**, při kterém dojde k fyzickému narušení zařízení za účelem přečíst z něj tajnou informaci

- **Neinvazivní**, při kterém není zařízení nijak fyzicky poškozeno. Do této skupiny spadají útoky postranními kanály jako např. výkonové, chybové a časové analýzy.

Invazivní útoky

Výrobce se snaží tento útokům čelit např. zalitím čipu do hmoty z epoxidové pryskyřice, či odstraněním typového čísla integrovaného obvodu, což má za následek znesnadnění identifikace použitého obvodu či přístupu k němu.



Obr. 2.3.4: Různé možnosti ochrany čipu: a) Zalitím do epoxidové pryskyřice, b) odstraněním typového čísla

Pakliže je integrovaný obvod zalit vrstvou epoxidu, máme tři možnosti, jak se k němu dostat či alespoň určit polohu komponentů v čipu:

- **Chemickou cestou** použitím speciální chemikálie k odstranění ochranné vrstvy (např. MG Chemicals' 8310 Conformal Coating Stripper) (viz lit. [16])

- **Fyzickou cestou** pomocí speciálního nářadí

- **Rentgenový paprsek** k zjištění polohy komponentů v čipu a spojů

Pakliže útočník získá přístup k integrovanému obvodu, může se pokusit přečíst z něj tajné informace (např. privátní klíče). Toho lze dosáhnout např. odposloucháváním dat na sběrnici, či vybroušením pouzdra integrovaného obvodu a za použití UV lamp, rentgenu aj. z něj pokusit přečíst informace.

Neinvazivní útoky

Cílem útoku není poškodit fyzicky dané zařízené, ale pouze sledovat, jak se chová při daných podmínkách a pokusit se dané chování využít k získání tajných informací.

- **Časová analýza** využívá toho, že čas kryptosystémů koreluje s hodnotami jejich soukromých klíčů. Obrana spočívá v tom, že zajistíme, aby měly operace náhodnou délku (např. přidáním šumu).

- **Chybová analýza** využívá toho, že různé chyby mohou snížit bezpečnost zařízení. Příkladem chybové analýzy může být např. sledování chování zařízení, necháme-li ho pracovat mimo pracovní podmínky specifikované výrobcem, např. při extrémních teplotách, či při zvýšeném napětí.

- **Výkonová analýza** umožňuje z příkonu čipové karty určit, jaké operace právě provádí.

2.4 Biometrická autentizace

Biometrická autentizace využívá jedinečných biologických znaků k autentizaci. Nejčastěji se jedná o otisk prstu, dalšími možnými prvky pro autentizaci jsou tvar ruky, sítnice, duhovka, tvar obličeje, či lidský hlas.

Biometrické systémy pracují na principu porovnávání výše uvedených znaků s již dříve uloženým znakem. Biometrické systémy je možné využívat v kombinaci s jinými autentizačními předměty, např. čipovými kartami SmartCard (např. model 330m), čímž dojde ke zvýšení bezpečnosti.

2.5 Zhodnocení autentizačních metod

Existují tři způsoby autentizace a to autentizace pomocí uživatelského jména a hasla, dále autentizace pomocí certifikátů a biometrická autentizace. Každý způsob má svoje výhody, ale i nevýhody.

Autentizace pomocí uživatelského jména a hesla je nejméně bezpečná, protože je možné heslo odchytit, odpozorovat, popřípadě získat některým známým útokem (viz tab. 2.5.1). Naproti tomu je tato metoda nejjednodušší a nejlevnější a za předpokladu, že uživatel použije bezpečné heslo, které je následně hashováno se solí, nabízí dostačující úroveň zabezpečení pro méně významné aplikace (např. internetová fóra).

Dalším způsobem je autentizace pomocí certifikátu. Tento způsob ve spojení s dvou faktorovou autentizací přináší vysokou míru zabezpečení, protože privátní klíč nelze z autentizačního předmětu nikterak získat a předmět sám o sobě nelze nijak zkopírovat. Nevýhodou daného řešení je riziko zcizení autentizačního předmětu a odhalení PINu pomocí keyloggeru. Tento problém lze eliminovat biometrickou autentizací, či kombinací biometrické autentizace a PINu. Další nevýhodou řešení jsou vyšší pořizovací náklady na čipové karty a

čtečky, popř. USB tokeny, proto je dané řešení vhodné pro kritické aplikace, jenž vyžadují vysokou bezpečnost (např. e-Banking, či vzdálený přístup do firemní sítě).

Posledním způsobem je za použití biometrických rysů člověka pro autentizaci. Tento způsob je velmi bezpečný, protože biometrické rysy nelze ukrást a pro uživatele též velmi jednoduchý, protože k autentizaci stačí např. pouhé přiložení prstu na snímač. Nevýhodou daného řešení je nepřesnost snímače v případě, má-li autentizující se osoba např. špinavé ruce, či špatně přiloží prst na snímač. Následující tabulka udává ucelený přehled vlastností autentizačních metod.

Tab. 2.5.1: Přehled vlastností autentizačních metod

Autentizační metoda	**Vlastnosti**
Autentizace pomocí uživatelského jména a hesla	Autentizace pomocí přihlašovacího jména a hesla představuje nejjednodušší a nejlevnější autentizační metodu. Z hlediska bezpečnosti nejméně bezpečnou. Výhody: • Jednoduché a levné řešení Nevýhody: • Heslo lze odpozorovat, či zachytit pomocí „keyloggeru“ • Nebezpeční prolomení hesla slovníkovým útokem. Ochranou proti tomuto útoku je tzv. solení haší. • V případě krátkého a jednoduchého hesla hrozí nebezpečí prolomení útokem hrubou silou.
Autentizace pomocí certifikátů	Autentizace pomocí certifikátů představuje bezpečný způsob autentizace. Výhody: • Kartu, či token nelze duplikovat. • Privátní klíč nikdy neopouští kartu, či token.

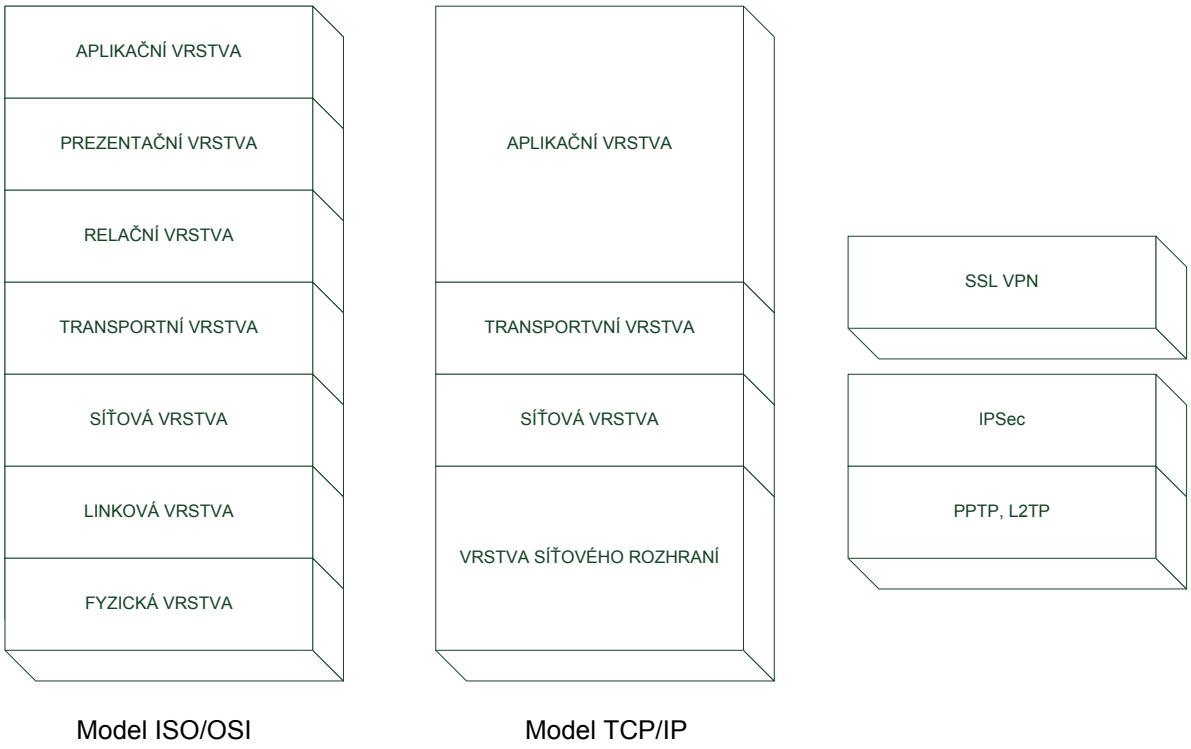
	Nevýhody: • PIN lze odpozorovat, či odchytit pomocí „keyloggeru“. Ovšem bez vlastnictví autentizačního předmětu nepodstatné. • V případě uložení privátního klíče do bezpečného úložiště operačního systému možnost zneužití v důsledku bezpečnostní chyby systému.
Biometrická autentizace	Biometrická autentizace využívá jedinečných biologických rysů k autentizaci. Jelikož biometrické rysy člověka (např. otisk prstu) nelze ukrást, nabízí tato varianta nejvyšší míru zabezpečení. Výhody: • Biologické rysy (např. otisk prstu) nelze ztratit, zapomenout, či ukrást. • Biometrikou lze nahradit PIN pro přístup k čipové kartě, nebo použít současně s PINem pro tří faktorovou autentizaci Nevýhody: • Za určitých okolností nepřesné snímání

3 VIRTUÁLNÍ PRIVÁTNÍ SÍTĚ

Virtuální privátní sítě umožňují provozování zabezpečené sítě přes veřejnou sít, jako je např. Internet (viz lit. [18]).

3.1 VPN technologie a protokoly

Existuje několik technologií VPN, které pracují na různých vrstvách modelu ISO/OSI, či TCP/IP.



Obr. 3.1.1: Technologie VPN na jednotlivých vrstvách modelů ISO/OSI a TCP/IP.

- **PPTP (Point to Point Tunelling Protocol)** je sítový protokol TCP/IP (viz lit. [7]), který využívá klasické Point-to-Point (PPP) relace s GRE zapouzdřením na TCP portu 47 a dále relace na TCP portu 1723 pro zahájení a řízení GRE relace. Je podstatně méně bezpečný, než protokol L2TP, protože jeho šifrovací klíče jsou odvozeny z hesla uživatele.

- **L2TP (Large Two Tunelling Protocol)** je novější sítový protokol podobný PPTP (viz lit. [8]), který je kompatibilní s ATM, Frame Relay, či X.25. Používá spojení UDP a lze v kombinaci s protokolem IPSec zajistit zcela bezpečné spojení.

- **SSL VPN (Secure Socket Layer VPN)** umožňuje komunikovat bezpečně po nezabezpečené síti, nepotřebuje klienta, pro přístup postačuje webový prohlížeč.

- **SSTP VPN (Secure Socket Tunneling Protocol)** je nový protokol společnosti Microsoft (viz lit. [9]), který využívá protokol SSL pro přenos PPP komunikace. Řeší tak problémy protokolů PPTP a L2TP v sítích zabezpečených branamy firewall, či při překladu adres (NAT).

- **IPSec (IP Security)** umožňuje komunikovat bezpečně po nezabezpečené síti.

Dále bych se chtěl zabývat podrobněji protokolem IPSec. IPSec je soubor protokolů pracujících na sítové vrstvě, který umožňuje zabezpečenou komunikaci. Pro přenos dat existují v IPSec dva mody – tunelovací a transportní. V případě tunelovacího modu se zašifrují veškerá data včetně záhlaví a přidá se nové IP záhlaví. V případě transportního modu jsou šifrována pouze data, hlavička zůstává nešifrovaná.

Obr. 3.1.2 Transportní mód

Obr. 3.1.3 Tunelovací mód

Protokoly IPSec:

- Bezpečnostní protokoly, jež zajišťují bezpečnost. Patří sem protokoly ESP, AH.
- Protokol pro bezpečnou výměnu klíčů IKE.
- Protokol pro bezpečnou výměnu klíčů a ustanovení bezpečnostních pravidel komunikace ISAKMP.

IPSec má dvě fáze:

- Hlavní mód (Main Mod).
- Rychlý mód (Quick Mod).

V režimu Main Mod se dohodnou bezpečnostní pravidla a dojde k ověření obou stran, které chtějí komunikovat a v Quick Modu pak probíhá výpočet samotného šifrovacího klíče a přenos dat.

Dále je důležité zmínit, že protokol IPSec nešifruje veškerou komunikaci. Mezi nešifrovanou komunikaci patří například multicast, IKE, ověření kerberosem aj.

3.2 Kategorie VPN

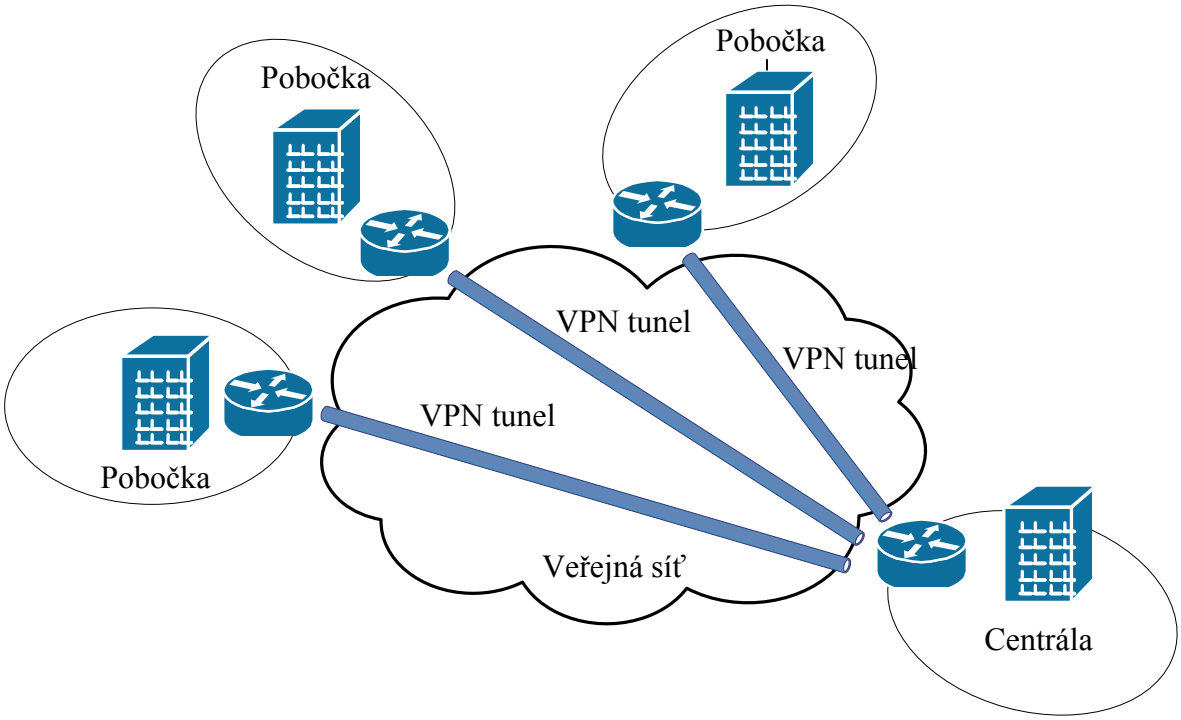
Virtuální privátní sítě VPN spadají do dvou kategorií

- **Site-to-Site**
- **Remote-Access**

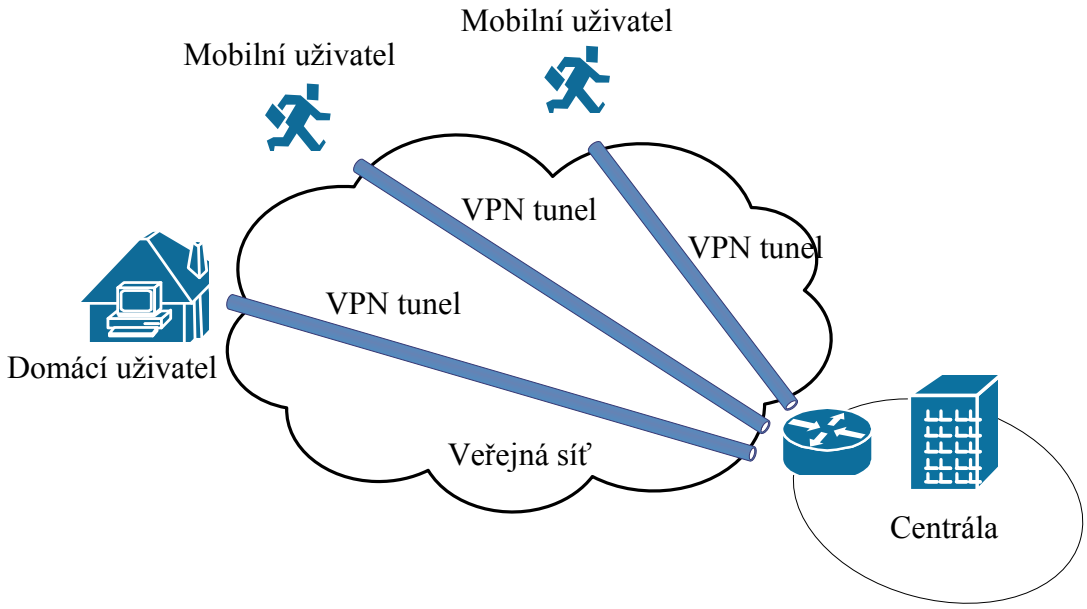
Site-to-Site VPN umožňuje propojení částí organizace, které se nalézají v odlišných geografických oblastech. Rozlišujeme 2 typy Site-to-Site VPN:

- **Intranet VPN** umožňuje spojení se vzdálenými pobočkami v rámci jedné organizace.
- **Extranet VPN** umožňuje spojení mezi organizacemi, např. mezi obchodními partnery, nebo zákazníky.

Remote Access umožňuje vzdáleným firemním pracovníkům přistupovat k serverům organizace a přitom využít infrastrukturu veřejné sítě (internet).



Obr. 3.2.1: Site-to-Site VPN



Obr. 3.2.2: Remote Access VPN

Průběh připojení Remote Access VPN:

1. Uživatel se připojí k ISP.
2. VPN klient (software) se připojí k serveru VPN dané organizace, ke které se chceme připojit. VPN dále inicializuje ověření.
3. Dojde k ověření uživatele, zajistí se zabezpečení podle daných pravidel.
4. VPN server pošle klientovi IP adresu a ten pak směruje daný provoz přes VPN. Veškerá komunikace přes VPN je šifrovaná, aby nemohl nikdo třetí odposlouchávat data.

Při navazování spojení VPN je důležité, aby byly obě strany důvěryhodné a tedy aby nebylo navázáno spojení s počítačem, který byl podvržen útočníkem. Proto se musí obě zařízení autentizovat. Existují 2 způsoby autentizace:

- **Pre-shared key (PSK)** jedná se o sdílená a manuálně přiřazená hesla, jejich využití je především při menším počtu VPN tunelů, při větším by to bylo administrativně velmi náročné.

- **Public-Key infrastructure (PKI)** v tomto případě je autentizace založena na certifikátech. Vzdálený uživatel a VPN server si u certifikační autority (CA) vyžádají certifikát, kterým se identifikují při navazování spojení. Pro případy zcizení klíče je možní v pravidelných intervalech generovat nové certifikáty.

3.3 Srovnání hardwarového a softwarového řešení VPN

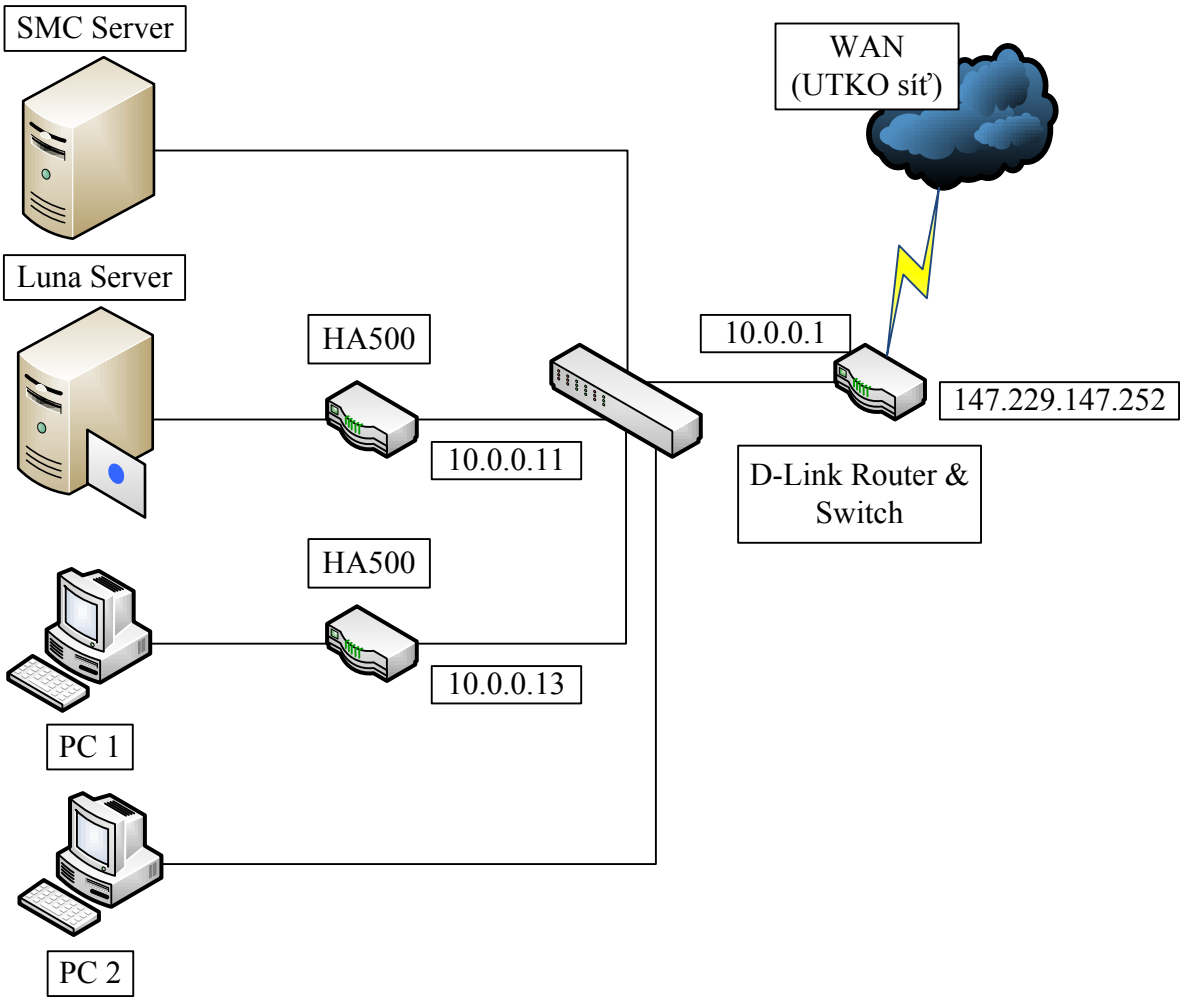
VPN lze realizovat dvěma způsoby, jednak softwarově a jednak hardwarově. Každá varianta má své pro i proti, rozhodneme-li se pro softwarové řešení, vynaložíme mnohem menší náklady na jeho realizaci, ovšem za cenu menší bezpečnosti. Serverový operační systém, na kterém VPN server poběží, je složitý a může obsahovat spoustu bezpečnostních chyb, které mohou zneužít jak viry, tak i útočníci. Dalším důležitým faktorem je výkon takového řešení, kdy při větším počtu uživatelů může dojít k vysokému zatížení serveru a jeho nedostupnosti. Proto se softwarové řešení VPN hodí v situaci, používá-li VPN menší počet uživatelů anebo jsme finančně omezeni.

Naproti tomu hardwarové řešení v sobě spojuje vysoký výkon a bezpečnost. VPN brány jsou osazeny výkonným kryptografickým čipem pro vysoký výkon kryptografických operací a mnohých případů je jeho bezpečnost zaručena certifikace FIPS 140-2. Jedinou nevýhodou tohoto řešení jsou vysoké pořizovací náklady a tak je toto řešení vhodné tam, kde je požadována vysoká bezpečnost a vysoký výkon.

4 NÁVRH KONKRÉTNÍHO ŘEŠENÍ KRYPTOGRAFICKÉHO ZABEZPEČENÍ LOKÁLNÍ POČÍTAČOVÉ SÍTĚ

V rámci bakalářské práce byla sestavena laboratorní síť (viz obr. 4.1), ve které je realizováno VPN spojení za pomoci technických prostředků firmy SafeNet, jenž je špičkou ve svém oboru.

Na stanicích je nainstalován SSO klient od společnosti SafeNet, který umožňuje využití čipových karet SmartCard a USB Tokenů pro autentizaci uživatelů pro přístup do vzdálené počítačové sítě chráněné hardwarovými VPN branami HighAssurance 500 Gateway. Dále je na stanicích nainstalován VPN klient SafeNet HighAssurance Remote, který umožňuje samotný vzdálený přístup do chráněné počítačové sítě. O centrální správu VPN bran se stará zvláštní server, na kterém běží aplikace Security Management Center, který je připojen na public porty VPN bran. O centrální správu čipových karet SmartCard a USB Tokenů se potom stará aplikace Administrative Management Center.



Obr. 4.1: Schéma zapojení laboratorní sítě

Tab. 4.1: Podrobné informace o počítačích a síťových prvcích laboratorní sítě

Název	Hardware	Software	IP adresy
Luna Server	Intel Xeon, 2GB RAM, Luna PCI 3000 (FW 4.5.3)	MS Win Server 2003 Std. EN SP2 AMC	LAN1: 192.168.0.2
SMC Server	Intel Xeon, 4GB RAM	MS Win Server 2003 Std. EN SP2 SMC v2.0 b 3159	LAN: 10.0.0.12
PC1	Intel Pentium D 512MB RAM	MS Win XP SP2 HA Remote v1.7.7 b 6	LAN: 192.168.1.2
PC2	Intel Pentium D 1GB RAM	MS Win XP SP2 HA Remote v1.7.7 b 6	LAN: 10.0.0.10
D-Link VPN Router	1x WAN, 4x LAN	-	WAN: 147.229.147.252/24 LAN: 10.0.0.1/24
SafeNet HA500 #1	2x LAN 1x RS232	-	LAN1: 10.0.0.11/24 LAN2:
SafeNet HA500 #2	2x LAN 1x RS232	-	LAN1: 10.0.0.13/24 LAN2:

4.1 Technické prostředky SafeNet

Společnost SafeNet nabízí nejrůznější prostředky pro zabezpečení sítí. Námi realizovaná sít disponuje hardwarovými VPN branami HighAssurance 500 Gateway, kryptografickým modulem Luna PCI 3000, USB Tokeny iKey 2032 a čipovými kartami SmartCard 330 Series. V následujícím textu se budu věnovat využití právě těchto prostředků.

4.1.1 Realizace VPN

Hlavním technickým prvkem při realizaci VPN byly brány HighAssurance Gateways, sloužící pro zabezpečení vzdáleného přístupu do počítačové sítě, dále softwarový VPN klient a o konfiguraci celého řešení se starala aplikace Security Management Center (SMC).
Vysokou míru zabezpečení celého řešení dokazuje certifikace FIPS 140-2, která se vztahuje jak na bránu, tak i na softwarového klienta.

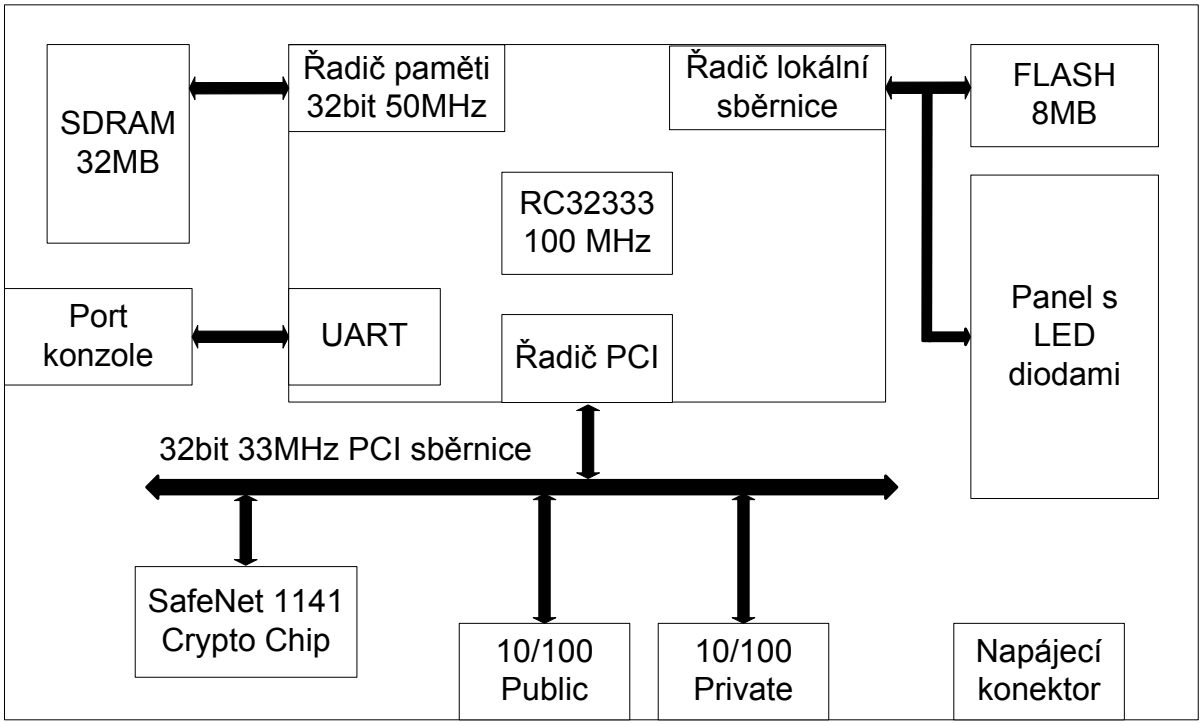
Hardwarové VPN brány

Společnost SafeNet nabízí několik modelů VPN bran, lišících se maximálními rychlostmi a vlastnostmi. Jednotlivé modely a jejich základní parametry jsou uvedené v tabulce 4.1.1.

Tab. 4.1.1 Základní parametry VPN bran HighAssurance Gateways

Model	Počet VPN tunelů	Propustnost (DES, 3DES, AES)	Využití	Délka klíče
HA500	500	1,5Mbps	Zabezpečení menších poboček	1024 bitů
HA1000	1000	10Mbps	Zabezpečení menších poboček	1024 bitů
HA2000	10 000	100Mbps	Zabezpečení regionální pobočky	1024 bitů
HA4000	1024	1Gbps	Zabezpečení centrálního sídla	2048 bitů

Jelikož v našem projektu byly použity brány s typovým označením HighAssurance 500 Gateway, budu se jim věnovat podrobněji (viz lit. [19], [20]). Srdcem VPN brány HA500/1000 je 32bitový mikrokontrolér IDT79RC32333, který je připojen na 32 bitovou sběrnici, ke které je též připojen kryptografický čip SafeXcel 1141, či novější SafeXcel 1741, který má na starosti veškeré kryptografické operace.



Obr. 4.1.1: Blokové schéma HighAssurance 500 Gateway.

Kryptografický čip SafeXcel 1741 slouží k akceleraci IPSec a zahrnuje následující kryptografické operace:

- Podpora IPSec
- Základní šifrovací, dešifrovací a hašovací funkce
- Operace s veřejným klíčem
- Operace náhodného generování čísel

Kryptografický čip zahrnuje také následující algoritmy nutné pro VPN:

- DES, 3DES, AES
- Hašovací funkce MD-5, SHA-1
- Operace s veřejným klíčem (Diffie-Hellman, RSA, DSA)
- Generátor náhodných čísel

Softwarový VPN klient

Dále se budu věnovat softwarovému klientovi VPN od společnosti SafeNet. VPN klient umořuje navázat VPN spojení se vzdálenou stranou, kterou může být VPN brána, či jiný klient. Firma SafeNet nabízí dva typy těchto klientů určených pro operační systémy Microsoft Windows a Sun Solaris:

- **Soft Remote** je VPN klient který je de facto celosvětovým standardem a využívají ho i jiné společnosti, např. Cisco.
- **HighAssurance Remote** má stejné možnosti jako SoftRemote s tím rozdílem, že používá knihovny certifikované dle FIPS 140-2.

Pro větší zabezpečení klientské stanice obsahuje VPN klient integrovaný firewall od společnosti ZoneLabs ZoneAlarm. Ten, jak jsme se přesvědčili, je dobré nevypínat, protože na internetu je dostupný exploit [2], který zneužívá chybu v knihovně IPSecDrv.sys pro DoS útok.

Správa a konfigurace VPN řešení SafeNet

Security Management Center (SMC) je aplikace, umožňující vzdálenou centralizovanou správu VPN bran HA500/1000/2000/4000. Aplikace je primárně vyvíjena pro operační systém Sun Solaris a s určitým časovým odstupem je k dispozici i port na operační systém Microsoft Windows. Veškerá komunikace mezi SMC a branami je šifrována, SMC využívá

protokoly SNMPv2/3 a Telnet. Součástí SMC je i interní certifikační autorita, ale je možné použít i externí, mezi podporované patří Entrust, iPlanet a Microsoft. V takovém případě je nutné do brány nahrát veřejný klíč dané CA. Námi použitá brána HighAssurace Gateway 500, ale i vyšší modely s výjimkou HighAssurance Gateway 4000 podporují pouze klíče o velikost max. 1024 bitů, což může mít negativní dopad na zabezpečení celé sítě. Model 4000 potom podporuje i klíče o délce 2048 bitů, což poskytuje dobrou míru zabezpečení.

Hlavní funkce SMC:

- Vzdálená konfigurace bran
- Správa pravidel pro VPN
- Interní CA
- Správa CRL

Po připojení bran do sítě je ve výchozím nastavení používána autentizace s předsdíleným klíčem. Chceme-li brány konfigurovat prostřednictvím SMC, musíme provést jejich certifikaci, k čemuž nám poslouží interní CA. Certifikace je poměrně snadná, k tomu, aby byla úspěšně dovedena do konce stačí znát pouze sériové číslo brány. U vyšších modelů může být vyžadován USB token dodaný spolu s branou. Nepoužíváme-li model 4000 je také nutné, aby byl server s aplikací SMC připojen k public portu brány a dále aby na serveru nebyla nainstalována jiná CA, jinak by certifikace skončila chybou. SMC dále umožňuje nastavit jednotlivá VPN pravidla a ty následně nahrát do vybraných VPN bran, což zefektivňuje jejich správu.

Možnosti realizace VPN spojení

- **Spojení mezi dvěma klienty** jedná se o nejjednodušší a nejlevnější řešení, protože není potřeba žádného dalšího hardwaru. Nejprve je třeba zvolit identitu vzdálené strany, tou může být IP adresa, doména + IP adresa, e-mail + IP adresa, podsít, rozsah IP adres, či jakákoli stanice. Dalším krokem je volba certifikátu. Pokud z nějakého důvodu nechceme použít certifikát, můžeme použít předsdílený klíč (PSK) o délce min. 8 znaků. Budeme-li chtít použít certifikát, musíme nejprve vytvořit v Certificate Manageru, který je součástí klienta, žádost o certifikát (Certificate Request). Zde můžeme také zvolit délku klíče, a zda li bude klíč vygenerován softwarově, nebo přímo v USB tokenu, či kartě Smart Card, což přináší nejvyšší možnou míru bezpečnosti klíče, protože nikdy neopustí hardware, ve kterém byl vygenerován. Po té, co je žádost vygenerována, musíme ji potvrdit certifikační autoritou. Zde máme na výběr mezi interní certifikační autoritou, která je součástí SMC anebo certifikační autoritou z Windows Serveru 2003, o jejíž bezpečnost se stará kryptografický modul Luna PCI 3000. Jakmile máme žádost potvrzenou od certifikační autority (Certificate Request Response File), importujeme ji do Certificate Manageru a máme podepsaný

certifikát s privátním klíčem, který můžeme použít pro VPN autentizaci. Aby byl námi vytvořený certifikát s klíčem považován za důvěryhodný, je nutné importovat certifikát od dané certifikační autority.

- **Spojení mezi klientem a branou** zapojí do VPN spojení i hardwarové VPN brány, což významným dílem přispěje k celkové bezpečnosti řešení. Abychom mohli uskutečnit spojení mezi klientem a branou, je nutné, aby byl v bráně nainstalován kořenový certifikát důvěryhodné CA. Dále je nutné vytvořit VPN pravidla, k tomu slouží VPN Policy Manger, který je součástí SMC. Tyto pravidla mohou definovat použité šifrovací algoritmy, TCP porty, které budou přes VPN dostupné a dále strany, které spolu budou komunikovat. V našem případě jsme zvolili komunikaci mezi jakýmikoli klienty a VPN branou, což je řešení vhodné pro větší společnosti, kde by bylo obtížné definovat jednotlivé uživatele.
  Konfigurace na straně klienta je obdobná v předchozím případě, liší se pouze v tom, že je nutné zadat IP adresu naší VPN brány. To se provede zatržením volby Use Secure Gateway Tunel a zadáním její IP adresy.

VPN brány umožňují mimo výše uvedené i spojení s klienty třetích stran (např. Cisco Systems) a spolupracují s branami jiných výrobců. Možné vzájemné propojení:

- HA500 – HA500
- SMC – HA500
- Gateways – HA500
- Softwarový klient – HA500

4.1.2 Autentizace pomocí technologie SafeNet

Abychom mohli realizovat výše uvedené VPN spojení je nutné ověřit uživatele, jenž chce přistupovat do vzdálené sítě. Kdybychom použili autentizaci prostřednictvím hesla, riskovali bychom jeho prozrazení, či prolomení a tím ohrozili bezpečnost naší sítě. Tento problém řeší využití infrastruktury veřejného klíče, pomocí kterého je možné mnohem bezpečnější ověřit vzdáleného uživatele (problematiku distribuce veřejného klíče jsem rozebral podrobněji v kapitole 1.5). Klíč potom může být uložen v bezpečném úložišti operačního systému, což nemusí být vždy dostatečně bezpečné, zvláště v případě, přihlašuje li se uživatel z domácího počítače. Řešením tohoto problémů může být zavedení čipové, nebo li také dvou faktorové autentizace za pomoci čipové karty SmartCard, či USB Tokenů.

Čipové karty SmartCard a USB Tokeny iKey společnosti SafeNet

Společnost SafeNet nabízí několik modelů čipových karet SmartCard a USB Tokenů, které se liší svými vlastnostmi. Tabulka 4.1.2 nám podává ucelený přehled dostupných karet společnosti SafeNet od základních až po specializované modely.

Tab. 4.1.2: Parametry jednotlivých karet SmartCard.

Model	Parametry
400	Nejvyšší model karet Smart Card od SafeNetu, podporuje standardy FIPS 201, FIPS 140-2 Level 2 a PIV-2.
330	Smart Card pro všeobecné použití
330m	Smart Card s podporou biometriky
330g	Smart Card GSA kompatibilní
330i	Spart Card pro Identrus Systém
330u	Smart Card s podporou „User PIN unblocking“

Při návrhu naší počítačové sítě byly použity modely 330m a 330u. Jejich hlavní rozdíl spočívá v podpoře biometriky, kterou je možno použít pro autentizaci.

Firma SafeNet nabízí také USB Tokeny a to pod označením iKey hned v několika verzích. V našem projektu byly použity USB Tokeny iKey 2032 pro VPN autentizaci a iKey 1000 pro autentizaci obsluhy kryptografického modulu Luna PCI. USB Token ikey 2032 je velmi podobný kartám SmartCard, obsahuje totiž stejný kryptografický čip jako SmartCard 330, který je připojen přes USB-to-Smart Card můstek na port USB. Některé modely, podporující FIPS 140-2 level 2 a vyšší, mají pouzdro z pryskyřice, které se při pokusu o vniknutí rozlomí na několik kusů a token je tak nenávratně zničen. Tabulka 4.1.3 porovnává jednotlivé modely tokenů iKey od SafeNetu.

Tab. 4.1.3: Přehled USB tokenů od SafeNetu.

Model	Paměť (kB)	Certifikace FIPS 140-2	Max. délka klíče	Algoritmy
1000/1032	8/32	-	1024	MD5, CHAP/HMAC
2032FIPS	32	Level 2	2048	RSA, DSA, DH, DES
3000	20	-	1024	RSA, MD5
4000	64	Level 3	2048	3DES, AES, DH, SHA-1

SafeNet Borderless Security

Jedná se o architekturu řešící problém bezpečnosti informačních technologií. Tato architektura v sobě kombinuje ověření, oprávnění a důvěrnost informací v jediném integrovaném řešení, pro všechny webové a newebové aplikace.

Borderless Security využívá metodu řízení přístupu Single Sign-On, která umožňuje na základě jediné autentizace přístup k velkému množství prostředků jako např. přihlášení do operačního systému, či k emailu přes webové i newebové rozhraní. Ke konfiguraci a správě USB Tokenů a karet SmartCard slouží nástroj Administrative Management Center (AMC).

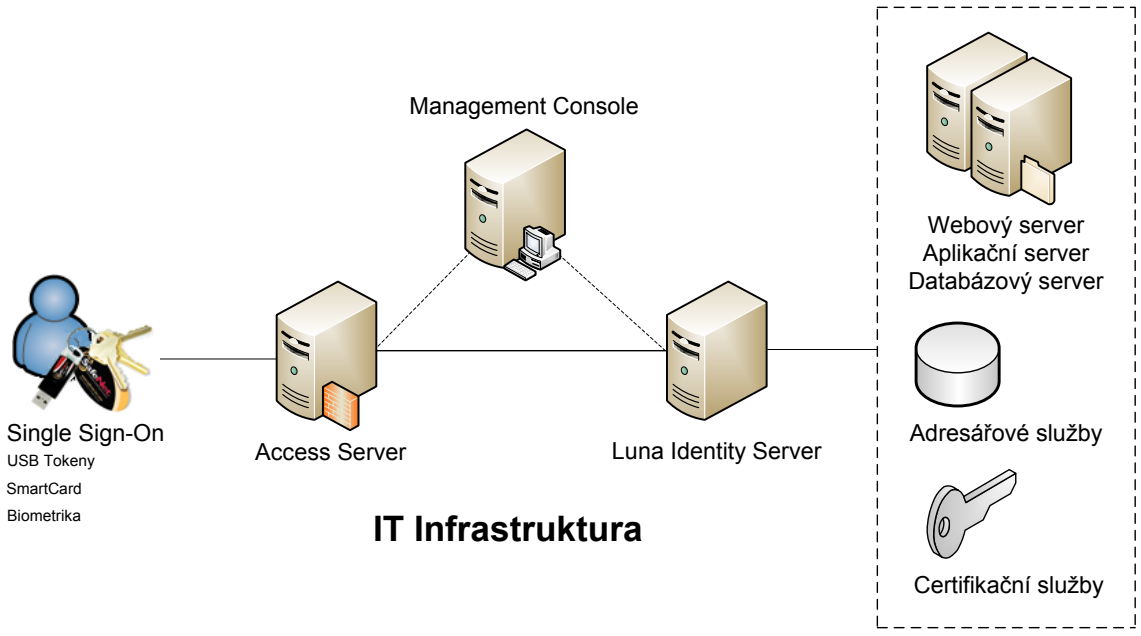
Celá platforma se skládá z následujících komponent:

- **Klient** jedná se o aplikaci, jež běží na uživatelském počítači a umožňuje využívat USB Tokeny, SmartCard či Biometriku pro autentizaci.

- **Přístupový server** (Access Server) umožňuje ověření vzdáleného uživatele a na jeho základě umožnit přístup ke vnitřním zdrojům firemní sítě prostřednictvím IPSec, či SSL VPN. Firma SafeNet dodává pro funkci přístupového serveru integrované řešení Borderless Security Access Server.

- **Management Console** slouží ke správě platformy Borderless Security. umožňuje odvolání či obnovení pověření přístupu, správu životního cyklu karet SmartCard, či USB Tokenů apod.

- **Pověřovací server** (Credential server) jedná se o volitelný prvek sítě, jenž zvyšuje bezpečnost. Má na starosti správu identit, které jsou chráněny interním kryptografickým modulem Luna PCI.



Obr. 4.1.2: Platforma SafeNet Borderless Security

V naší laboratorní síti není využita celá architektura SafeNet Borderless Security, nýbrž pouze část – Borderless Security SSO, jenž má na starosti autentizaci uživatelů pomocí autentizačních předmětů

Technologie Single Sign-On

Technologie Single Sign-On (SSO) nám umožňuje přístup k několika prostředkům na základě jediné autentizace. SSO můžeme využít k systémové autentizaci, či aplikační autentizaci. (např. přihlášení do Windows, přihlášení k emailu přes webové i newebové rozhraní apod.) Technologie SSO nachází uplatnění v případě, chceme li zavést velmi přísnou bezpečnostní politiku, např. složitá hesla, která by si uživatel nezapamatoval. Ke konfiguraci SSO slouží nástroj Administrative Management Center (AMC). AMC umožňuje vytvoření předkonfigurovaného klienta, který je distribuována na klientské počítače a umožňuje využívat USB Tokeny a karty SmartCard ve spojení s technologií SSO. AMC existuje ve třech verzích, jejichž základní funkce jsou stejné a liší se pouze v doplňkových funkcích:

- S podporou SSO a biometriky
- S podporou SSO
- Bez podpory SSO (dodává se zdarma k USB Tokenům)

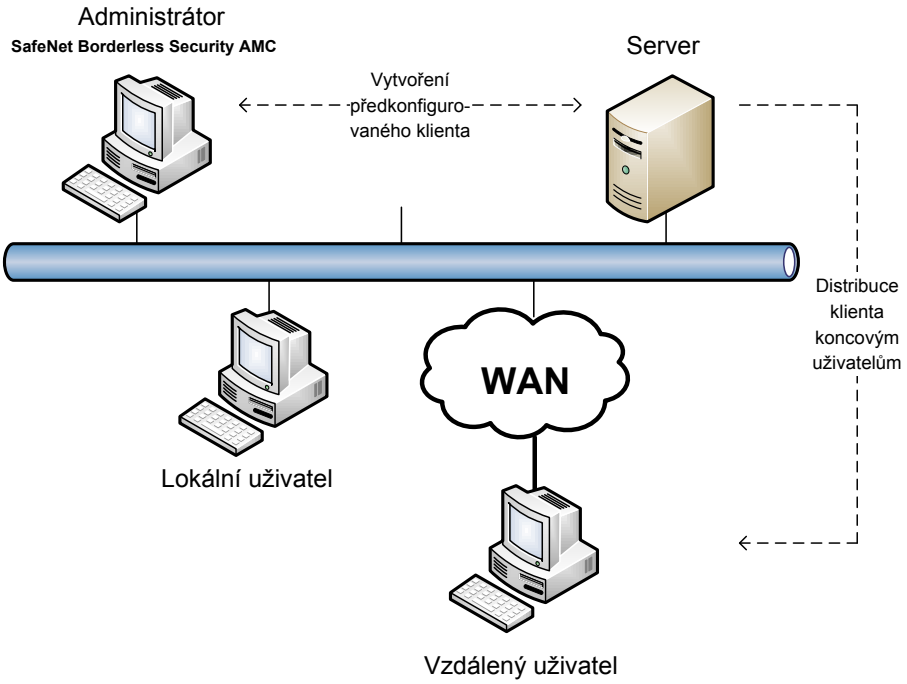
AMC se skládá z následujících částí:

- **Token Manager**, který umožňuje nastavení parametrů karet a USB tokenů, jako je např. složitost PINu, maximální počet špatně zadaného PINu, délka PINu a v případě, že máme zakoupenou licenci, můžeme použít k autentizaci i biometriku.

- **Policy Manager**, který umožňuje nastavení pravidel pro jednotlivé aplikace, či přihlašovací dialogy Internet Exploreru.

- **Client Builder**, který umožňuje vytvoření instalačního balíku klienta dle zvolených parametrů, např. použití certifikátů, podpora DSA, možnost importu P12 certifikátů, žádost o certifikát, či jeho obnovení, lokální a vzdálené přihlášení k Windows apod.

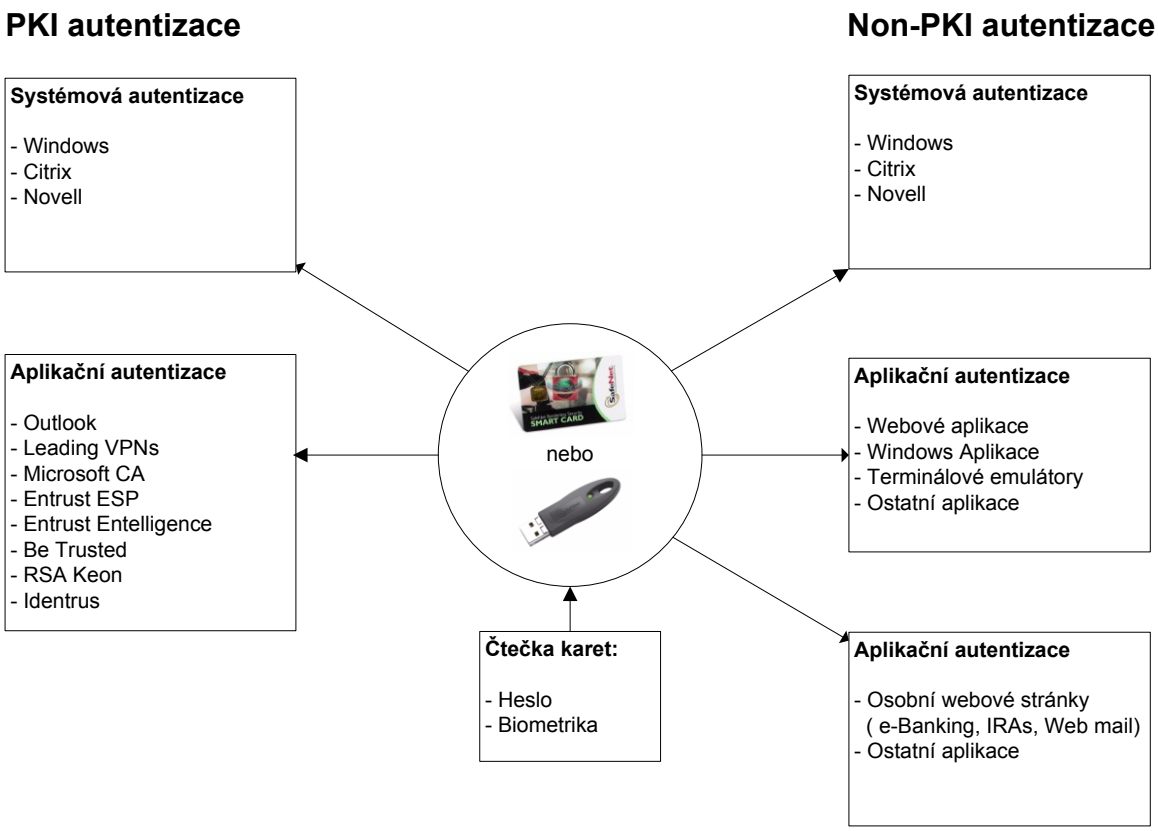
Prvním předpokladem nasazení SafeNet Borderless Security SSO je vytvoření předkonfigurovaného klienta, který se nazývá Policy Client, který je následně distribuován koncovým uživatelům. Těchto předkonfigurovaných klientů můžeme vytvořit hned několik dle předpokládaného použití určitou skupinou pracovníků.



Obr. 4.1.3 Distribuce klienta koncovým uživatelům

Tento klient potom umožňuje používat USB Tokeny, karty Smart Card, či biometrickou autentizaci k následujícím činnostem:

- Zabezpečení E-Mailové komunikace a webových transakcí
- Přihlašovací dialog Windows
- Zabezpečení VPN
- Podpora Single Sign-On (SSO)
- Zabezpečení non-PKI informací



Obr. 4.1.4: Možnosti využití Borderless Single Sign-On (SSO)

4.1.3 Kryptografické moduly SafeNet

Firma SafeNet je jedním z největších výrobců kryptografických modulů, a to jak jednoúčelových, tak i sítových. Mezi jednoúčelové kryptografické moduly patří Luna PCI, Luna CA3/CA4, mezi sítové zase Luna SA, Luna SP. Přesnější popis jednotlivých HSM popisuje Tab. 4.1.4. Naše CA je chráněna kryptografickým modulem Luna PCI 3000, kterému se budu podrobněji věnovat.

Tab. 4.1.4: Srovnání některých modelů HSM Luna

Typ	Provedení	Výkon	Typické využití
Luna SA	Network-Attached HSM	4000 transakcí/s	Ochrana privátního klíče a akcelerace kryptografických operací
Luna CA3	Dedicated HSM	25 1024bit RSA podpisů/s	Ochrana privátního klíče kořenové CA, bezpečné zálohování
Luna PCI	Dedicated HSM	7000 1024bit RSA operací/s	Ochrana privátního klíče CA a akcelerace kryptografických operací.
Luna PCM	Dedicated HSM	-	Funkce zálohovacího média (ve spojení s Lunou CA3)

Luna PCI 3000 je jednoúčelový kryptografický modul, podporující normu FIPS 140-2 Level 2 a jeho vysoký výkon dokazuje schopnost zvládnout 3000 asymetrických 1024 bitových RSA operací za sekundu. Pro zabezpečený přístup k soukromému klíči CA nabízí modul dvou-faktorovou autentizaci založenou na rolích. Ke kryptografickému modulu je připojena speciální klávesnice PED (Pin Entry Device) s jedním portem USB, do kterého je připojen speciální USB Token (iKey 1000), který je chráněn PINem. USB token slouží k autentizaci uživatele, který s jeho pomocí získá přístup k privátnímu klíči CA uloženém v kryptografickém modulu. Tabulka 4.1.5 popisuje jednotlivé role pro přístup ke kryptografickému modulu.

Tab. 4.1.5: Operační role pro přístup ke kryptografickému modulu Luna PCI 3000

Určení	PED klíč	Operační role	Funkce
Administrátorské	HSM Admin SO	Security Offices	Administrace tokenů/HSM, Nastavení bezpečnostních pravidel pro tokeny, výběr inicializačních parametrů tokenů, tvorba uživatele.
	Domain	Domain Cloning Token Backup	Sada klonovacích pravidel, tvorba/přenos kopie domény, záloha tokenů.
Každodenní použití	User Partition owner	User	Generování klíčů, podepisování, dešifrování.
	M of N	M of N	Sdílené tajemství M z N, M klíčů z N požad. k ověření

4.2 Konfigurace autentizačních prvků sítě

Nyní bych se chtěl věnovat konfiguraci jednotlivých prcků sítě, které souvisejí s autentizací. Nejprve se budu věnovat konfiguraci SSO klienta a následně přejde ke konfiguraci kryptografického modulu Luna PCI a certifikační autoritě.

4.2.1 Konfigurace Borderless Security SSO

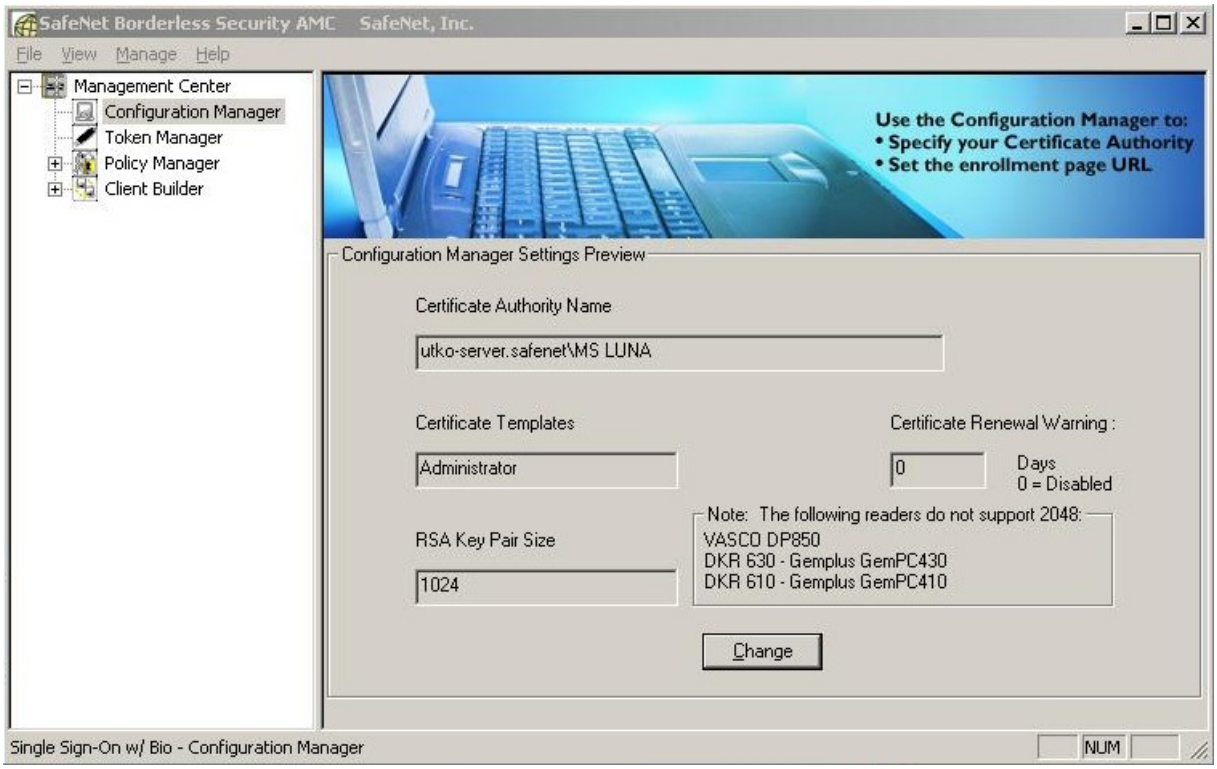
Ke konfiguraci Borderless Security SSO slouží aplikace Administrative Management Center (AMC). Hlavní okno AMC obsahuje čtyři zákožky, pomocí kterých je možné konfigurovat PKI, upřesňující parametry autentizace pomocí tokenu, či karet, nastavení pravidel pro SSO a možnost konfigurace klienta s přesně definovanými parametry.

Obr. 4.2.1 Úvodní obrazovka SafeNet AMC

Configuration Manager

V této záložce provádíme konfiguraci certifikační autority, pakliže chceme využívat PKI.

- **Certificate Autority Name**: Jméno certifikační autority včetně sítové cesty. Pokud nechceme využívat PKI, necháme prázdné.
- **Certificate Template**:
  - *SmartCardLogon* – Chceme-li využít USB Token, či kartu využít pro přihlášení do systému.
  - *SmartcardUser* – Chceme-li využít USB Token, či kartu využít pro přihlášení do systému a pro bezpečnou emailovou komunikaci.
- **Certificate Renewal Warning**: Varování před vypršením platnosti certifikátu.
- **RSA Key Pare Size**: velikost klíče (512 bit, 1024 bit, 2048 bit)



Obr. 4.2.2: Konfigurační okno Certification Manageru

Token Manager

Token Manager umožňuje nastavit parametry pro autentizaci prostřednictvím tokenu, či karty. Mezi základní možnosti nastavení patří:

- Maximální počet chybných pokusů o přihlášení (Maximum Failed Login Attempts): Udává, kolikrát je možné zadat špatné heslo. Počet špatně zadaných hesel je 4-10, poté bude token zablokován.
- Minimální délka hesla (Minimal Passphrase Length): Minimální délka hesla 4-8 znaků.
- Hodnota vypršení platnosti tokenu (Token Timeout Value): Udává dobu, za kterou bude nutné znovu zadat heslo pro přístup k tokenu. Hodnota se pohybuje v rozmezí 0-240 minut.

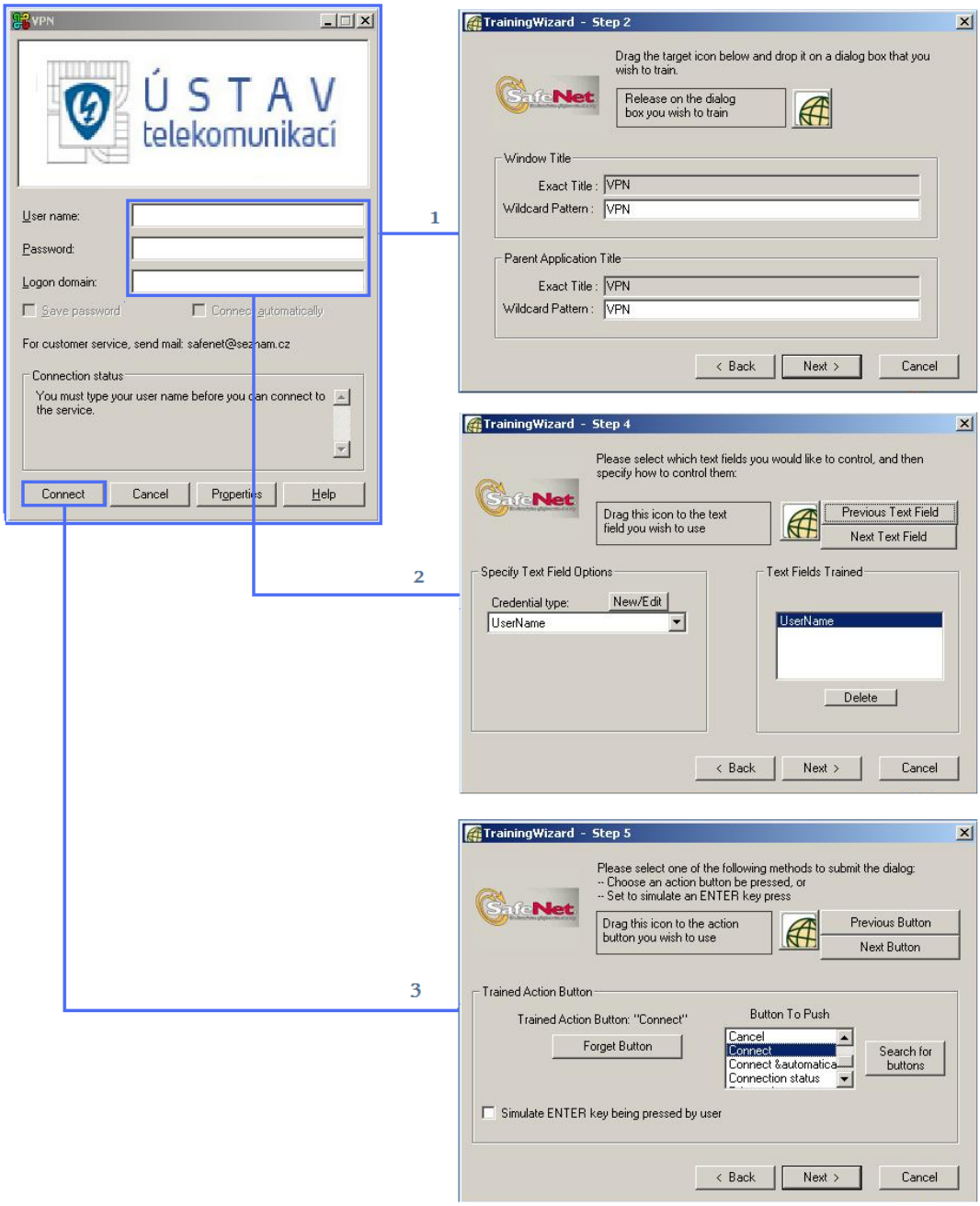
V případě využívání biometriky máme možnost nastavit citlivost a dále, zdali budeme vyžívat pouze biometriku, či kombinaci PINu a biometriky.

Policy Manager

Policy Manager umožňuje uložení hesel z přihlašovacích dialogů aplikací, či www stránek na token pro využití SSO. Uživatel potom zadá PIN pro přístup k tokenu a přihlašovací dialogy budou automaticky vyplněny a odentrovány, takže si uživatel nemusí pamatovat

žádné heslo a je sníženo riziko jeho zcizení. Výhodou je možnost využití skupin, která ulehčuje správu většího množství uživatelů.

Konfigurace SSO



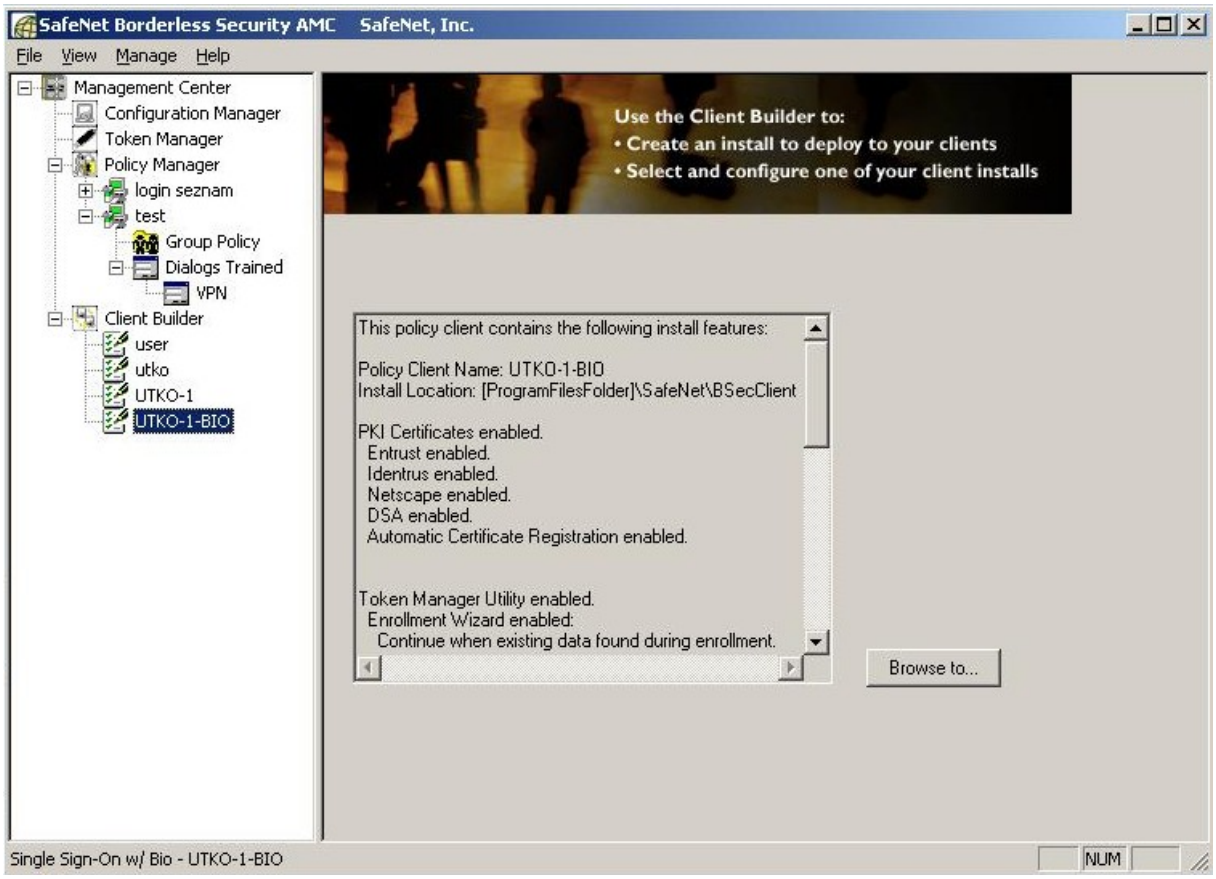
Obr. 4.2.3: Konfigurace SSO

Nejprve pomocí speciálního kurzoru vybereme okno aplikace, ve které se nalézá přihlašovací dialog (1), následně pomocí stejného kurzoru vybereme políčko – uživatelské jméno, které v průvodci vyplníme, stejný postup opakujeme pro heslo (2). V posledním kroku budeme vyzváni k výběru tlačítka, které se má automaticky zmáčknout po vyplnění

přihlašovacích údajů. V průvodci se nám zobrazí seznam dostupných tlačítek, ze kterých vybereme tlačítko connect (3). Popisek vybraného tlačítka se změní na select, potvrdíme volbu forgett button a tím je průvodce SSO ukončen.

Client Builder

Umožňuje tvorbu klientské aplikace podle předdefinovaných pravidel. Lze definovat jaké PKI certifikáty budou použity a zdali budou automaticky obnoveny, dále lze definovat CSP pro naši kartu, či token, podporu biometriky (je-li zakoupena licence) apod.



Obr. 4.2.4: Dialogové okno tvorby klienta

Po definování všech pravidel vyexportujeme instalační soubory kliknutím na tlačítko Browse to a zadáním cesty. Toho je pak možno distribuovat jednotlivým klientům.

4.2.2 Konfigurace kryptografického modulu Luna PCI

Abychom mohli kryptografický modul použít, musíme nainstalovat jeho ovladače a dále poskytovatele kryptografických služeb LUNA CSP, který nám umožní využívat modul pod operačním systémem Microsoft Windows Server 2003. Abychom mohli modul používat,

musíme jej nejprve inicializovat a následně na něm vytvořit oddíl. K tomu slouží konzolový konfigurační nástroj LunaCM.

Inicializace modulu

1) Nejprve připojíme čistý USB Token (PED Key) do PED

2) Z příkazového řádku Microsoft Windows spustíme konfigurační nástroj LunaCP, který jsme nainstalovali.

3) Zadáme příkaz „hsm init“ a zadáme název pro náš modul.

   Příklad:

   lunacm:> hsm init -label nazev_modulu

   Budeme upozorněni, že inicializujeme modul a všechna data na něm budou zničena, na konci procesu budeme vyzváni, abychom vložili PED Key do PED.

   You are about to initialize the HSM.
   All contents of the HSM will be destroyed.
   Are you sure you wish to continue?

   Type 'proceed' to continue, or 'quit' to quit now -> proceed

   Please attend to the PED.

   Na displeji PED budeme upozorněni, že jsme vložili prázdný PED key a že se na něj chystáme zapsat klíč pro autentizaci HSM Admina.

   Slot 1
   Initialize HSM
   WARNING
   This PED Key is blank
   Overwrite YES/NO

   Potvrdíme stiskem tlačítka Yes a zadáme heslo o délce minimálně 7 číslic. O úspěšné inicializaci a vytvoření role HSM Admina se můžeme přesvědčit příkazem „hsm showinfo“

Vytvoření oddílu

1) Nejprve se přihlásíme k modulu jako HSM Admin. Vložíme HSM Admin PED key do PED. V příkazovém řádku zadáme příkaz „hsm login“, a na PED zadáme heslo a potvrdíme volbu.
2) Nyní se můžeme pustit do tvorby oddílu příkazem „partition create“.

lunacm:> partition create

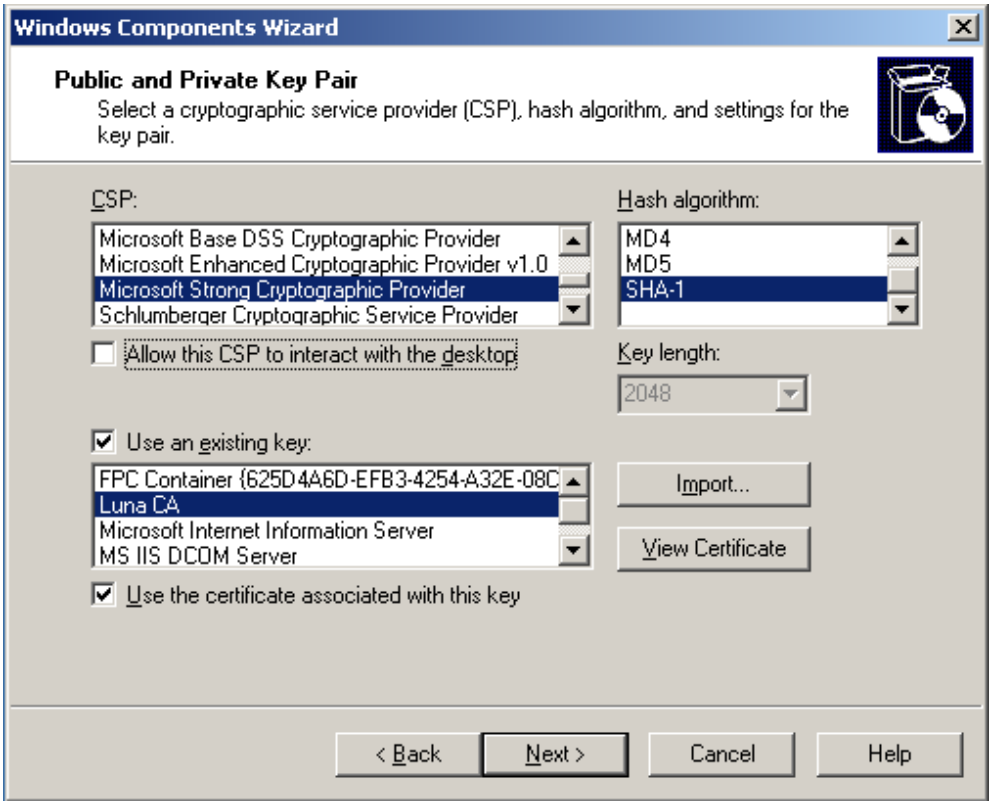
Please attend to the PED.

Vložíme do PED prázdný PED Key a vytvoříme uživatele Partition Owner stejným způsobem, jako jsme vytvořili HSM Admina.

Nyní, když jsme modul inicializovali a vytvořili na něm oddíl, provedeme jeho registraci v operačním systému Microsoft Windows Server 20003 pomocí konzolového nástroje „register“ který spustíme s parametrem „/partition“. Tím je hardwarový kryptografický modul Luna PCI připraven k použití.

4.2.3 Konfigurace CA s využitím Luna PCI

Nejprve je nutné nainstalovat CA na náš server, to provedeme přidáním součásti systému „Certificate Service“ pomocí nástroje přidat, nebo odebrat programy v prostředí Microsoft Windows. Hned na začátku instalace zvolíme volbu rozšířené volby a v následujícím dialogovém okně vybereme poskytovatele kryptografických služeb Luna CSP, zvolíme délku klíče 1024 bitů (pozn. Literatura [3] doporučuje použít v případě kořenové CA délku klíče 2048 bitů, my ovšem kvůli kompatibilitě s hardwarovými VPN branami zvolili kratší délku klíče), dále hashovaní algoritmus SHA-1. Pokud provádíme reinstalaci CA, můžeme použít existující klíč.

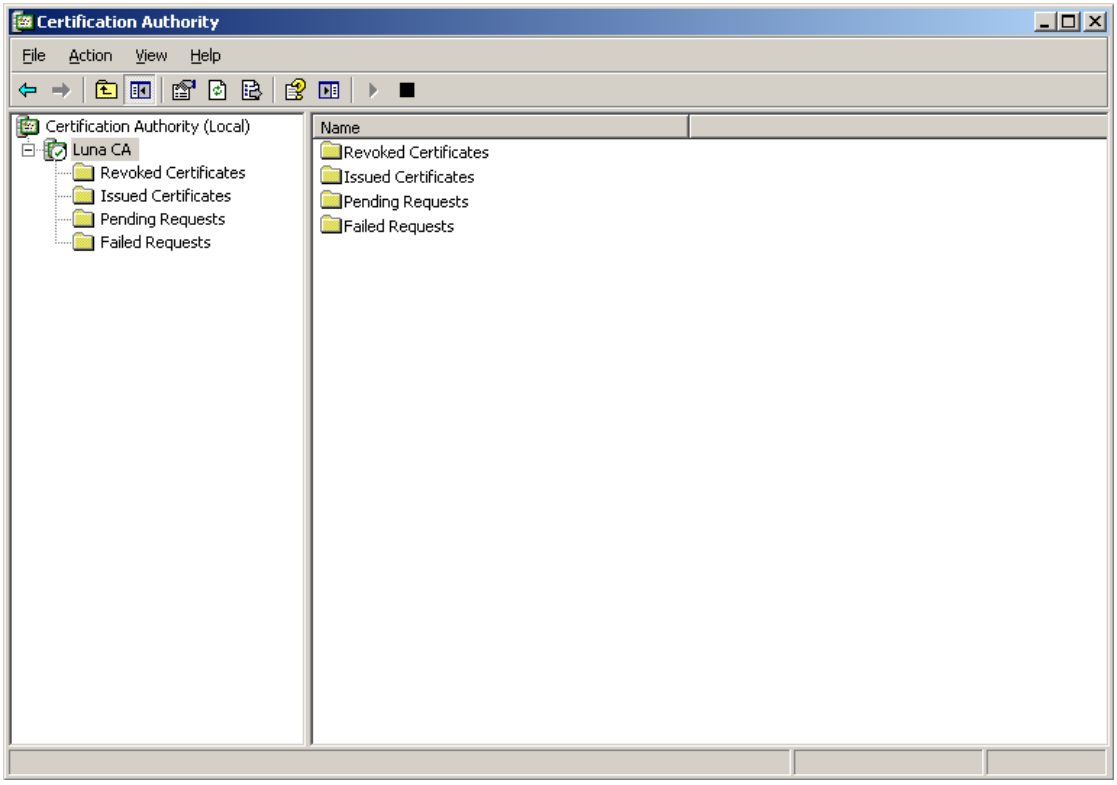


Obr. 4.2.5: Dialogové okno instalace CA – Výběr CSP a ostatních nastavení

Před samotným generováním klíčového páru naší CA vložíme uživatelský PED Key do PED, zadáme heslo a potvrdíme, v tomto okamžiku jsme získali přístup k modulu, na který se uložil vygenerovaný klíč.

V následujícím dialogovém okně budeme dotázáni, jaký typ CA chceme instalovat, a na délku platnosti klíče. V našem případě standalone kořenová CA. Tím je instalace naší CA u konce.

Nyní můžeme přistoupit k využívání služeb naší CA. Spustíme Microsoft Management Consoli (MMC) a přidáme do něj modul „Certification Authority“.



Obr. 4.2.6: Okno MMC s modulem Certification Authority

Využití služeb CA si provedeme na příkladu, ve kterém potvrdíme žádost o vydání certifikátu (Certificate regest).

1) V klientské aplikace (v našem případě se bude jednat o VPN klienta SafeNet HighAssurance Remote) vytvoříme žádost o vydání certifikátu.

2) V MMC konzoli pro konfiguraci CA klikneme pravým tlačítkem myši na certifikační autoritu Luna CA a v nabídce „All task“ zvolíme položku „Submit new certificate request“, následně se nám otevře okno pro výběr souboru, který se nám uloží do složky „Pending Requests“

3) Nyní přistoupíme k samotnému procesu vydání certifikátu. Na žádost klikneme pravým tlačítkem myši, dáme volbu „Issue“. Vložíme náš uživatelský PED Key do PED, zadáme heslo a potvrdíme. Certifikát vydaný naší CA nalezneme ve složce „Issued Requests“.

4) V našem VPN klientovi nyní certifikát importujeme a můžeme jej použít k ověření totožnosti.

ZÁVĚR

Tématem této práce jsou kryptografické moduly pro zabezpečení sítí. První tři kapitoly tvoří teoretickou část práce. První kapitola se věnuje obecně základům moderní kryptografie.

Druhá kapitola se zabývá autentizací, jež využívá kryptografických prostředků uvedených v předchozí kapitole. Jsou tu popsány některé sítové autentizační protokoly. Kapitola se věnuje použitím digitálních certifikátů, které umožňují dnes nejbezpečnější způsob autentizace a dále autentizačním předmětům, jako jsou čipové karty a USB tokeny.

Tématem třetí kapitoly je zabezpečení počítačových sítí pomocí technologie VPN. Kapitola udává ucelený přehled o jednotlivých typech VPN a na závěr podává zhodnocení softwarové a hardwarové implementace této technologie.

Praktickému použití technologií uvedených v předešlých kapitolách se věnuje čtvrtá kapitola. Ta je věnována konkrétnímu řešení kryptografického zabezpečení lokální počítačové sítě pomocí technologií firmy SafeNet, jenž patří k nejlepším ve svém oboru.

Laboratorní počítačová síť je chráněna hardwarovou VPN branou, která umožňuje vzdálený přístup autentizovaným uživatelům do lokální sítě. Autentizace jednotlivých uživatelů je založena na digitálních certifikátech, které jsou z bezpečnostních důvodů popsaných v práci, uloženy na autentizačním předmětu. O vydávání digitálních certifikátů se stará certifikační autorita chráněná hardwarovým kryptografickým modulem, která tvoří nedílnou součást celé architektury.

Důkazem vysoké bezpečnosti celé architektury je certifikace FIPS 140-2, která se vztahuje jak na hardwarové, tak i na softwarové prostředky laboratorní sítě.

Nevýhodou řešení je vysoká cena, která je mimo jiné dána i certifikacemi, které jsou velmi drahé. Další nevýhodou je podpora pouze dvou operačních systémů a to Sun Solaris a Microsoft Windows. S podporou Linuxu se v mnoha případech nepočítá, taktéž podpora 64 bitových operačních systémů je zatím omezená. Nevýhodou je také nedostatek dokumentace, což je vykompenzováno placenou podporou, která ovšem tvoří další náklady. V těchto ohledech mají výhodu open source řešení, které jsou zdarma, nabízejí nespočetné množství dokumentace, ale podpora tvořená pouze komunitou nemusí být vždy dostačující.

Na závěr kapitoly jsem se věnoval konfiguraci autentizačních prvků sítě, nastínil jsem, jak nastavit SSO klienta pro použití autentizačních předmětů a dále jak zprovoznit hardwarový kryptografický modul a jeho využití ve spojení s certifikační autoritou.

LITERATURA

[1] DOSEDĚL, T.: *Počítačová bezpečnost a ochrana dat*, Computer 2004, ISBN 80-251-0106-1

[2] SAFENET HIGH ASSURANCE REMOTE 1.4.0 (IPSECDRV.SYS) REMOTE DOS [online]. 2007 [cit. 23.4.2008]. Dostupný z WWW: <http://securitydot.net/xpl/ exploits/ vulnerabilities/articles/1830/exploit.html>

[3] KOMAR, B.: *Microsoft Windows Server 2003 PKI and Certificate Security*. MS Press 2004, ISBN 0-7356-2021-0

[4] WIKIPEDIA: *FIPS 140* [online]. Dostupný z WWW: <http://en.wikipedia.org/wiki/ FIPS_140>

[5] KIAER, M.: *Multifactor authentication in Windows – Part 1: Smart Cards and USB Tokens*. 2007. Dostupný z WWW : <http://www.windowsecurity.com/articles/ Multifactor-authentication-Windows-Part1.html >

[6] WIKIPEDIA: *SSL* [online]. Dostupný z WWW: < http://cs.wikipedia.org/wiki/SSL>

[7] MICROSOFT TECHNET: *PPTP* [online]. Dostupný z WWW: <http://technet2.microsoft.com/windowsserver/cs/library/bed19640-544d-461a-9167-d7955d8f73551029.mspx?mfr=true >

[8] MICROSOFT TECHNET: *L2TP* [online]. Dostupný z WWW: <http://technet2.microsoft.com/windowsserver/cs/library/bed19640-544d-461a-9167-d7955d8f73551029.mspx?mfr=true>

[9] DAVIES, J.: *The Cable Guy The Secure Socket Tunneling Protocol* [online]. 2008 [cit. 21.5.2008]. Dostupný z WWW: < http://technet.microsoft.com/en- us/magazine/ cc162322.aspx>

[10] MICROSOFT TECHNET: *IPSec* [online]. [cit. 20.2.2008] . Dostupný z WWW: <http://technet.microsoft.com/en-us/library/bb726946.aspx>

[11] SAFENET INC.: HSM SafeNet [online]. [cit. 15.12.2007]. Dostupný z WWW: <http://www.safenet-inc.com/products/pki/index.asp>

[12] SAFENET INC.: *Smartcard SafeNet* [online]. [cit. 15.12.2007]. Dostupný z WWW: < http://www.safenet-inc.com/products/tokens/products_sc.asp>

[13] CHMELA, L. *Kerberos – strážce podsvětí*. Časopis Connect! 10/2001

[14] CISCO SYSTEMS, INC.: *Protokol 802.1X*. [online]. 2005 [cit. 8.3.2008]. Dostupný z WWW: < http://www.cisco.cz/index.sub.php?pid=zpravy&typ=media&select=preview&id=59&tree=on>

[15] WEBER, F.: *Zabezpečení sítě proti neoprávněnému přístupu pomocí funkce NetworkLogin 802.1x* [online]. 2007 [cit. 8.3.2008]. Dostupný z WWW: <http://www.svetsiti.cz/view.asp?rubrika=Technologie&clanekID=313>

[16] MG CHEMICALS.: *Conformal Coating Stripper 8310* [online]. Dostupný z WWW: < http://www.mgchemicals.com/products/8310.html>

[17] GRAND, J.: *A historici Look at Hardware Token Compromises* [online]. 2004 [cit. 8.3.2008] . Dostupný z WWW: < http://www.blackhat.com/presentations/bh-usa-04/bh-us-04-grand/grand_hardware_token_US04_handouts.pdf>

[18] DAVIES, J., LEWIS, E.: *Deploying Virtual Private Networks with Microsoft Windows Server 2003*. MS Press 2004. ISBN 0-7356-1576-4

[19] NIST: *SafeNet HighAssurance 500/1000 Gateway Cryptographic Module* [online]. 2005 [cit. 8.3.2008]. Dostupný z WWW: < http://csrc.ncsl.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp385.pdf >

[20] SAFENET INC.: *SafeNet HighAssurance 500 Gateway* [online]. [cit. 8.3.2008]. Dostupný z WWW: < http://www.safenet-inc.com/products/gateways/ha500.asp >